现代数学译丛 1

椭圆曲线

及其在密码学中的应用—导引

〔德〕Andreas Enge 著

吴铤 董军武 王明强 译



TN918.1/37

2007

现代数学译丛 1

椭圆曲线及其在密码学中的应用——导引

〔德〕Andreas Enge 著

吴 铤 董军武 王明强 译

科 学 出 版 社

北 京

图字：01-2006-3955 号

内 容 简 介

本书以介绍椭圆曲线在密码学中的应用为目标，用浅显易懂的语言全面讲述了椭圆曲线公钥密码的相关知识，包括公钥密码学概述、有限域上椭圆曲线的算术理论、椭圆曲线上离散对数的求解算法以及有限域上椭圆曲线的求解算法等.

本书最突出的特点在于只利用近世代数等基础知识来揭示椭圆曲线内在的代数和几何结构，所以特别适合作为研究生和高年级本科生等初学者了解、掌握椭圆曲线公钥密码理论的入门书籍，也可供相关研究人员参考.

Translation from the English language edition:
Elliptic Curves and Their Applications to Cryptography
By Andreas Enge
Copyright © Kluwer Academic Publishers
Kluwer Academic Publishers is a part of Springer Science+Business Media
All Rights Reserved

图书在版编目(CIP)数据

椭圆曲线及其在密码学中的应用——导引/(德)恩格(Enge, A)著；吴铤，董军武，王明强译. —北京：科学出版社，2007
(现代数学译丛)
ISBN 978-7-03-020034-1

I. 椭… II. ①恩… ②吴… ③董… ④王… III. 椭圆曲线-应用-密码-理论
IV. TN918.1

中国版本图书馆 CIP 数据核字(2007) 第 174763 号

责任编辑：陈玉琢 莫单玉 / 责任校对：陈玉凤
责任印制：赵德静 / 封面设计：王 浩

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2007 年 12 月第 一 版 开本：B5(720×1000)
2007 年 12 月第一次印刷 印张：11 1/2
印数：1—3 000 字数：212 000

定价：38.00 元

(如有印装质量问题，我社负责调换<长虹>)

译者的话

随着计算机技术、网络技术，特别是 Internet 技术的飞速发展和广泛普及，人类社会已经进入了信息化时代. 如何在开放的网络环境中实现信息的保密性、完整性、可用性、可控性以及抗抵赖性已经成为了人们关注的焦点问题. 可以说信息安全问题已经成为制约信息化进程的主要瓶颈之一. 现代密码学作为解决信息安全问题的主要手段，其重要性得到了广泛认同.

自 1949 年, Shannon 发表的《保密通信的信息理论》将密码学研究纳入科学轨道以来，现代密码学基本可分为以 DES 为代表的对称密码学和以 RSA 为代表的公钥密码学. 由于公钥密码体制的非对称结构，从而在一定程度上克服了对称密码体制需要利用秘密通道来传递密钥这一弱点. 同时也正是由于其非对称结构，使公钥密码学不仅可以应用于数据加密，还可以被广泛地应用于身份识别、数字签名、密钥协商和电子支付等诸多领域，所以自 1976 年 Diffie 和 Hellman 提出公钥密码思想以来，公钥密码就引起了人们的广泛重视，在现代密码学中占据重要地位.

根据公钥密码体制所基于的数学难题来分类，目前有以下三类系统被认为是安全有效的：基于大整数分解问题的 RSA 型公钥密码；基于有限域上离散对数问题的 ElGamal 型公钥密码; 基于椭圆曲线离散对数问题的椭圆曲线公钥密码. 与其他公钥密码体制相比，椭圆曲线公钥密码体制突出的优势在于：对于其所基于的数学难题 —— 椭圆曲线离散对数问题 —— 目前并不存在亚指数时间算法，从而能够以更小的密钥尺寸来满足相同的安全性要求. 通常认为，为得到合理的安全性，RSA 应当使用 1024 比特的模长，而对于椭圆曲线密码体制，只需要使用 160 比特的模长. 而较小的密钥尺寸又带来了运行速度快、存储空间小、传输带宽要求少等诸多优点，这些优点使其特别适用于计算能力、存储能力、带宽受限，但又要求高速实现的应用领域，例如智能卡、无线通讯等. 椭圆曲线密码体制的以上优点使其受到国际上的广泛关注，这已经对 RSA, ElGamal 等公钥密码体制形成强劲的挑战.

另一方面，椭圆曲线公钥密码是以有限域上椭圆曲线的深刻理论为基础，涉及了包括代数数论、代数几何等许多数学分支，这给椭圆曲线公钥密码的普及与应用带来了一定的困难. 本书作者以椭圆曲线的密码应用为目标，通过浅显易懂的语言全面介绍了椭圆曲线公钥密码的相关理论. 本书的一个显著特点是：学习本书只需要大学里介绍的近世代数知识，而利用这些基础知识, 本书揭示了椭圆曲线内在的代数和几何结构，同时通过本书的学习就可以了解目前最新的研究进展，从而适合

作为信息安全研究人员，特别是研究生和高年级本科生等初学者了解、掌握椭圆曲线公钥理论的入门书籍.

本书的第 1 章对公钥密码学进行了概述性的描述；第 2 章介绍了椭圆曲线上的群运算法则，并揭示了其与除子类群之间的内在联系；第 3 章详细介绍了有限域上的椭圆曲线；第 4 章介绍了离散对数问题的各种求解方法，包括针对椭圆曲线离散对数问题的 MOV, Xedni 等多个攻击方法；第 5 章在重点介绍椭圆曲线点数计算方法 ——Schoof 算法的同时，描述了 SEA 算法的基本思想以及计算流程.

原书的序言、前言和第 1 章由王明强翻译，第 2 章、第 3 章、第 4 章由吴铤翻译，第 5 章由董军武翻译. 同时译者根据原书勘误说明对原书进行了相应的修改. 在本书的翻译过程中，得到了清华大学王小云教授以及译者同学的帮助，特此感谢！由于译者的专业知识和外语水平所限，书中错误与不妥之处在所难免，敬请读者批评指正.

本书的翻译和出版得到了国家“973”项目 (项目编号：2007CB807900, 课题编号：2007CB807902) 的资助，特此感谢！

译　者

2006.10.24

序　言

自 1976 年 Diffie 和 Hellman 提出公钥密码算法以来，许多公钥密码方案应运而生. 在通常情况下，几乎所有方案的安全性都是基于数学上的"困难"问题. 特别是大整数分解以及离散对数问题是几个最著名方案的安全核心.

公钥密码技术正广泛地应用于网上电子支付、无线股票交易以及在智能卡上的应用等多个商业安全领域. 其中比较著名的是 RSA 方案与 DSA(数字签名算法). RSA 的安全性基于大整数分解问题，而 DSA 的安全性则基于有限域乘法群中的离散对数问题. 以上这两个问题都存在亚指数时间算法. 这意味着在实际应用中为了获得足够的安全性，所使用的密钥长度必须超过 1000 比特. 由此可见，在能耗、存储空间以及带宽受限的许多应用领域中，就无法利用以上的技术来建立实用的公钥密码体制.

1985 年，Neal Koblitz 与 Victor Miller 独立地提出了椭圆曲线密码算法. 该算法的安全性是基于有限域上椭圆曲线点群中的离散对数问题. 到目前为止，求解椭圆曲线离散对数问题的最佳算法是指数时间算法. 由此就可以用较小的密钥长度来达到与原来相同的安全性要求, 从而可以将椭圆曲线密码算法应用于上述的受限应用领域. 经过过去十几年的发展，椭圆曲线密码算法已经得到广泛的应用, 并且诸如 ANSI, IEEE 与 ISO 等机构正在将椭圆曲线密码算法进一步地加以标准化. 在 1999 年 1 月, DSA 的椭圆曲线版本 (ECDSA) 成了美国金融机构的 ANSI9.62 标准.

椭圆曲线密码算法是以有限域上椭圆曲线的深刻理论为基础. 据我所知，很少有书介绍这些基本理论, 而以密码学应用为目的来介绍这些基本理论的书就更少了. 在本书中，Andreas Enge 用简单透彻但是易懂的语言介绍了这些基本理论. 在为高年级的本科生讲授椭圆曲线密码课时，我就用了这本书的初稿作为教材我也曾鼓励他将书稿出版. 现在，我为 Andreas 出版这本书而感到高兴. 我坚信对于那些想研究有限域上的椭圆曲线理论及其在密码学上的应用的人来说，本书是一本非常好的入门书籍.

S. A. Vanstone

前　言

在过去的 20 年里，公钥密码体制的诞生连同计算机科学技术的出现为一直以来都被看作是 “纯粹” 数学分支的数论和代数几何开创的一个新的应用领域. 椭圆曲线是现代密码学中最有发展前途的工具之一. 这进一步引起了数学工作者以及关注新密码算法实现的工程师和计算机科学家对这一领域的研究兴趣.

我们的目标是为那些学习椭圆曲线一般理论的读者提供一本入门教科书，为进一步学习更深刻的理论知识打下基础. 学习这本书只需要大学里讲授的近世代数知识. 读者只需了解多项式环、域的扩张和有限域的基本理论，通过本书的学习就能了解到目前最前沿的研究课题，如椭圆曲线上点的个数问题. 这个问题直到最近几年才被完全解决.

虽然椭圆曲线的其他应用，如大整数分解或素性证明，只涉及素域上的椭圆曲线，但是在密码学中特别感兴趣的是特征值为 2 的情况. 本书着重于对椭圆曲线进行一般性的描述，兼顾了特征值为奇数或偶数的情况，并且只有当需要的时候才对特征值的不同情况加以区分.

这里要非常感谢的是 Reinhard Schertz，正是他在大学里精彩的讲座引起了我对椭圆曲线的兴趣. 还要感谢 Dieter Jungnickel，是他建议我研究这个课题并且指导我完成了论文，并以那篇论文为基础最终形成了本书. 感谢 Leonard Charlap 与 David Robbins，他们精彩的报告是这本书的基础. 同时非常感谢 Marialuisa de Resmini 与 Scott Vanstone，正是由于他们的鼓励，才使本书得以出版. 在此还要对 Drik Hachenberger, Dieter Jungnicked, Charles Lam 与 Berit Skjernaa 说声谢谢，他们阅读了本书的初稿并且提出了很多有益的建议.

希望读者在阅读本书时能像我在写本书时那样获得很多乐趣.

Anderas Enge

目　　录

第 1 章　公钥密码算法

随着电子网络在现代经济社会中的广泛应用，密码学的应用已不局限于专门的军事和保密机构，而成为了一个公众关注的话题，诸如 UNO ([UNCITRAL, 1998a] 和 UNCITRAL [1998b]) 与 EU ([Commission of the European Communities, 1998]) 等国际组织也对密码学的应用表示出高度的关注. 与传统的密码相比，公钥算法应用范围更加广泛. 利用公钥算法大体上就可以实现世界上任何两人之间安全、可信的通信. 在下面的章节中，我们简要介绍公钥密码学的许多概念与基本思想, 并给出一些具体算法. 我们将着重介绍加密和数字签名的体制. 这些体制可以被推广到任意群上，特别是可以推广到椭圆曲线的点群上. 文献 [Stinson, 1995] 和 [Menezes et al., 1997] 对密码算法有综合全面的论述.

1.1　私钥密码学与公钥密码学

密码学是一门在一个公开信道上传递信息的艺术，其应当至少满足保密性与真实性这两个基本安全性要求. 保密性意味着即使攻击者能够窃听到所传送的信息，他也不能恢复出相应的明文消息；而真实性意味着消息发送者的身份与所发送消息的完整性是可以验证的. 我们首先讨论如何实现保密性，在 1.4 节我们对消息的真实性加以论述.

一般来说消息都以数字化的形式通过电子网络进行传送，如电子邮件、协议以及技术计划书、软件甚至人的声音等. 为了防止攻击，确保发送消息内容的安全，原始数据必须首先通过数学运算将其变成随机的形式，然后再加以传送.

因此，第一步是将消息转化成某种数学形式. 一般地，它们将被分成固定长度的组，每一组又被转化成一个整数或者一个比特串. 这一编码过程只是一种技术上的处理，它不能确保消息的安全. 对这一过程我们不做详细的描述，我们仍然称转化后的组为“消息”.

第二步是用某种方式将每组数据进行进一步的转化，使得未经授权者不能恢复出原始数据. 转化后的数据传送至指定的接受者，该接受者进行逆转化并按一定的规律重新组合恢复出原始数据. 粗略地来说，这种数据转化的算法就形成了一个密码系统.

严格来讲，一个密码系统由三个有限集合 $\mathcal{M},\mathcal{C}$ 和 $\mathcal{K}$ 以及一族*加密函数* $f_k:\mathcal{M}\to\mathcal{C}$ 构成，其中 $\mathcal{M},\mathcal{C},\mathcal{K}$ 分别表示*明文空间*、*密文空间*以及*密钥空间*，$k\in\mathcal{K}$. 换句话说，$\mathcal{M}$ 就是前面所说的原始数据集合，$\mathcal{C}$ 就是转化后的数据集合. 为了使加密和解密成为可能，f_k 必须能够有效计算并且是单射. 在许多情况下，$\mathcal{M}=\mathcal{C}$ 且 f_k 是双射.

当 Kevin 想给 Laura 发送一个秘密消息 $m\in\mathcal{M}$ 时，他首先选择一个密钥 $k\in\mathcal{K}$，然后计算*密文* $c=f_k(m)$ 并且将该密文通过一个可能不安全的信道发送给 Laura. Laura 必须对密文 c 应用加密函数的逆函数 ——*解密函数* f_k^{-1}，以获得原始消息 $m=f_k^{-1}(c)$.

在通常的*私钥密码系统*中，f_k 或者 f_k^{-1} 与密钥 k 是等价的. 这意味着一个有能力加密的人也能完成解密，反之亦然. 因此上面的方法有两个方面的主要缺陷：

密钥分发问题　任何两个想进行秘密通信的成员必须事先确定一个共同的密钥. 为此就必须事先通过一个安全信道来交换该共同密钥，例如他们可以事先见面商量，抑或使用一个可信赖的信使或者其他安全的方法. 该安全信道的建立往往要比用来传递后续消息的不安全信道要昂贵得多. 同时为了保证通信有较高的安全性，就必须经常改变这个密钥. 而这就增加了整个系统的运行成本. 与此同时，在一个有多个成员的网络中，整个系统的密钥数量大致是该系统成员数量的平方. 这样就会给密钥管理带来极大的麻烦.

签名问题　为了确保通过电子网络达成的协议的合法性，秘密消息的接收者必须能够向第三者 (如法官) 证明发送者的身份. 由于在传统的密码系统中，一个能解密密文的人也能加密任意的消息，因此对接受者来说，伪造一个自主选择消息的密文是没有任何问题的.

1976 年, Diffie 与 Hellman 提出了解决这些问题的一个方法. 该方法的提出给密码学带来了革命性的影响 [Diffie and Hellman, 1976]. Diffie-Hellman 的方法是以所谓的*单向函数*为基础，或者更精确地说是*单向陷门函数*. 假如每一个密钥 k 对应的加密函数 f_k 满足 "即使别人知道 f_k，他也是不可能计算 f_k^{-1}"，那么 Kevin 就能公布他的加密函数，即所谓的*公钥*. 这样任何人 (包括 Laura) 都能发送秘密的消息给 Kevin. 但是此时即使是 Kevin 也不能解密他收到的密文，这就限制了该密码体制的用途 (但是这种体制广泛应用在身份鉴别的协议中，身份鉴别一般存储一个加密口令). 这就是需要引入陷门函数的原因：对于单向陷门函数 f_k 来说，只要知道*秘密密钥*或者是*陷门* k，就很容易从 f_k 出发确定 f_k^{-1}. 如果 Kevin 知道密钥 k，那么他就能解密他所得到的密文.

这种处理办法解决了上面所述的两个问题：分发密钥时不再需要秘密信道. 相

反我们须将公钥发布在一个显著的地方以便两个陌生人之间实现保密通信. 如果 Kevin 想对一个发送给 Laura 的消息 m 进行签名 (这个消息可能是他们之间合同的一部分), Kevin 首先将解密函数 f_k^{-1} 作用在 m 上, 然后将 $(m, f_k^{-1}(m))$ 发送给 Laura. 由于 Kevin 是唯一知道解密函数 f_k^{-1} 的人, 因此 Laura 能通过比较 m 是否与 $f_k(f_k^{-1}(m))$ 相等来向任何第三方证明 $(m, f_k^{-1}(m))$ 的确来自于 Kevin. 如果所发送的消息还需要保密的话, 就可以用 $c = f_l(m)$ 来代替 m, 其中 f_l 是 Laura 的公钥.

文献 [Diffie and Hellman, 1976], p.648 中用诸如 "易于计算" 或者 "计算不可行" 这种非正式的语言来描述单向陷门函数, 除此以外对于单向陷门函数似乎不存在一个一般的可以接受的定义. 当我们系统地阐述这种函数所要满足的最低要求时, 就会看到产生这一问题的原因是明显的. 因为在复杂度理论中我们假设 "易于计算" 就是 "可以利用确定性算法在多项式时间内完成计算", 那么知道密钥 k 就可以在多项式时间内确定 f_k 和 f_k^{-1}. 同时如果已知函数 f_k 和 f_k^{-1}, 就可以在多项式时间内完成 $f_k(m)$ 和 $f_k^{-1}(c)$ 的计算. 另一方面, 即使已知 f_k(由此对任意的 m, $f_k(m)$ 就是已知的), 也不可能在多项式时间内确定 f_k^{-1} 或 $f_k^{-1}(c)$. 但是满足这些合理需求的单向陷门函数是否存在还是不确定的: 很明显存在一个非确定性的多项式时间算法来求 $f_k^{-1}(c)$, 也就是猜测一个 m 并且验证 $f_k(m) = c$ 是否成立. 如果利用确定性算法在多项式时间内可解的问题与利用非确定性算法在多项式时间可解的问题是一致的话, 即 $P = NP$, 那么就不存在单向陷门函数. 而 $P = NP$ 是否成立, 这是复杂性理论的一个重要的公开问题.

在实际应用中, 单向陷门函数满足即使在计算能力非常有限的情况下也能在 "合理的" 时间完成计算的函数, 而利用目前已知的最佳算法, 在计算能力非常强的情况下也不能在合理的时间内计算出它的逆函数. 当然这个定义服从于用户需要. 保密机构可以采用与个人用户不同的标准. 目前已经设计出许多单向陷门函数, 我们将在下面几节中介绍其中的几个.

在应用加密函数时, 经常会对 $\mathcal{M}$ 或者 $\mathcal{C}$ 中的数学对象进行运算. 由于指定消息的接受者在接到消息时必须对其进行逆变换, 因此数学对象的这些基本运算也应具有类似的性质. 一般地, 我们选择 $\mathcal{M} = \mathcal{C}$ 为群或者是只有极少数元素不可逆的幺半群 (通常来说, 元素的不可逆性将导致密码体制被破解, 因此这种情况发生的概率必须是可忽略的). 这里我们只对群的情况进行讨论, 并且在下面各节中用一般乘法群中的符号对算法进行描述, 因此椭圆曲线上的点群只是其中一种特殊情况.

1.2 Diffie-Hellman 密钥交换协议

密钥交换协议是 Diffie 和 Hellman 设计的. 该算法还不完全是公钥密码算法,

Diffie 和 Hellman 将其归类为“公钥分配协议”([Diffie and Hellman, 1976], p.468). 这个协议的思想是在不安全的信道上只交换部分信息，以使后来双方能共享一个共同的密钥. 同时即使攻击者碰巧获得这个部分信息，其也不能构造出这个共享的密钥. 该共享密钥能被用在传统的密码体制之中. 具体描述如下：

1. Kevin 与 Laura 公开地选择一个循环群 G 及其生成元 α . (在原始文献里 G 就是有限域的乘法群.)
2. Kevin 与 Laura 分别随机地选择整数 k 和 l 作为各自的密钥. 然后分别计算 α^k 和 α^l 并交换计算结果.
3. Kevin 与 Laura 利用各自获取的信息以及各自的密钥计算

$$\alpha^{kl} = (\alpha^k)^l = (\alpha^l)^k,$$

α^{kl} 就是共享的密钥.

注意到 α 的幂次甚至是较高的幂次都能够通过“平方–乘”算法得以有效地计算.

算法1.1 (“平方–乘”算法)　*设 α 是群中的一个元素并且 k 是一个自然数. 下面算法用 $O(\log k)$ 次群运算就能计算出 $\gamma = \alpha^k$.*

1. 令 $\gamma = 1$.

2. 重复下面的步骤直到 $k = 0$.

3. 如果 k 是奇数，则用 $k-1$ 代替 k, $\gamma\alpha$ 代替 γ, 这样总可假设 k 是偶数. 用 $\frac{k}{2}$ 代替 k, α^2 代替 α.

证明　在这个算法的运行过程中，值 $\gamma\alpha^k$ 是一个不变量，因此当 $k=0$ 时 γ 包含所要的结果. 这就证明了这个算法的正确性. 如果 k 的两进制表示长度是 r, 也就是 $2^{r-1} \leqslant k < 2^r$, 并且 $s \leqslant r$ 表示非零比特的个数，那么该算法恰好需要 $r-1$ 次平方运算和 $s-1$ 次乘法运算. 由此我们就给出了该算法的复杂度证明. □

当这个群是交换群时，在上面算法中我们可以用加法符号代替乘法符号，那么“平方 - 乘”算法就变成了双倍加算法. 这种算法早在古埃及时期就在整数乘法计算中使用, 参见 [Gillings, 1972].

一个窃听者在获取 Diffie-Hellman 密钥交换协议中传递的信息之后，如果想要恢复出密钥的话，就要从 α, α^k 和 α^l 中计算出 α^{kl}. 这个问题是著名的 Diffie-Hellman问题 . 求解该问题的一个明显方法是从 α^k 中计算 k, 这就是计算以 α 为底的 α^k 的离散对数 . 注意到 k 是在模 G 的阶的意义下是确定的，只要知道满足 $\alpha^{k'} = \alpha^k$ 的 k' 就能计算 $\alpha^{kl} = (\alpha^l)^{k'}$.

虽然到目前为止，不知道 Diffie-Hellman 问题与离散对数问题计算上是否等价，但是人们广泛认为这一结论应该是正确的. (实际上, 对于很大一部分有限群来说, Maurer 与 Wolf 已经证明它们之间的等价性, 参见 [Maurer and Wolf, 1996].) 如果等价的话，Diffie-Hellman 体制的安全性就是建立在离散对数问题困难性的基础上. 离散对数问题的困难性也与群的表示方法有关：如果模 n 的循环群 $G=(\mathbb{Z}_n,+)$ 被表示成 $\{0,\cdots,n-1\}$ 并且 $\alpha=1$，那么离散对数问题的求解是容易的. 我们将在第 4 章介绍离散对数问题. 要注意的是对于利用多项式或者正规基表示的有限域的乘法群，目前还不存在求解离散对数问题的多项式算法.

1.3 ELGAMAL 密码体制

在 Diffie-Hellman 密钥交换协议的基础上，ElGamal 在文献 [ElGamal, 1985] 中设计了一个真正意义上的公钥密码体制. 设 G 是循环群，α 为其生成元；$\mathcal{M}=G$, $\mathcal{C}=G\times G$. 每一个成员各自选择一个私钥 $a\in\mathbb{Z}$ 并公布 α^a. 假设 Kevin 希望传送一个消息 m 给 Laura.

1. Kevin 随机选择一个整数 k 并查看 Laura 的公钥 α^l.
2. Kevin 计算 $\alpha^{kl}=(\alpha^l)^k$，并发送 $(\alpha^k,m\alpha^{kl})$ 给 Laura.
3. Laura 利用自己的私钥 l 计算 $\alpha^{kl}=(\alpha^k)^l$ 并由此恢复出消息 m.

这个体制显然与 Diffie-Hellman 密钥交换协议等价. 这里以通过公开 α^l 的方式减少了一次数据的交换. 该体制的一个缺点是*消息扩展率为 2*：为了将群中某个一个元素所蕴涵的信息传送给对方，就必须传递两个群元素. 如果 Kevin 在每次发送消息时都使用同一个公钥 α^k，那么这种情况就可以避免，即 Kevin 只要传送这个公钥 α^k 一次即可. 但是这种简化有一个安全缺陷：如果偷听者已知某一组消息 - 密文对 $(m_1,m_1\alpha^{kl})$，他就可以针对下一个密文 $m_2\alpha^{kl}$ 通过计算

$$m_2=m_1\frac{m_2\alpha^{kl}}{m_1\alpha^{kl}}$$

恢复出明文 m_2. 一个合理的折衷方案是每一次 “会话” 时都采用不同的密钥 k. 而一次会话 (如 e-mail) 内容通常都由几个连续的信息 $m_1,m_2,\cdots,m_n$ 组成，这样加密后的数据由 α^k 和 $m_1\alpha^{kl},m_2\alpha^{kl},\cdots,m_n\alpha^{kl}$ 组成，从而将消息扩展率降为 $1+\frac{1}{n}$.

注意到与 1.1 节介绍的一般概念相比，在该体制中有一点是不对称的，从而使得签名变得不可能：因为 Laura 可以自己任意选择一个 α^k 或利用 Kevin 的公钥 α^k，来生成任意明文 m 的有效密文. ElGamal 有一个不同的签名方案，我们将在下一节加以阐述.

1.4 签名方案

在这一节里, 我们给出几个重要的签名方案，其具有前面所述的性质. 假设 Kevin 想发送一个签了名的消息 m 给 Laura, 那么他利用自己的密钥 k 以及明文, 在 m 上附加上一个 "签名". Laura 通过验证这个签名来证明 Kevin 是真正的发送者, 并且消息在发送过程中并没有被篡改过.

ElGamal 签名方案

文献 [ElGamal, 1985] 在给出加密体制的同时，提出了如下的签名方案. 其安全性依赖于群 G 上的 Diffie-Hellman 问题，其中 G 是以 α 为生成元的循环群. 假设 $g : \mathcal{M} = G \to \{0, \cdots, |G|-1\}$ 是一个可有效计算的双射, m 为待签明文. Kevin 的私钥与公钥分别是 k 和 α^k.

签名

1. Kevin 随机选择一个与 $|G|$ 互素的整数 k', 并且计算 $r = \alpha^{k'}$.
2. Kevin 求解同余方程

$$g(m) \equiv kg(r) + k's (\mathrm{mod}\, |G|). \tag{1.1}$$

由于 k' 与 $|G|$ 互素, 因此同余方程存在唯一解 $s \in \{0, \cdots, |G|-1\}$.

3. 签名就是数对 $(r, s) \in G \times \mathbb{Z}_{|G|}$, 该签名数对与 m 一起被发送给 Laura.

验证签名

1. Laura 根据 Kevin 的公钥 α^k 以及 m, r, s, 计算 $\alpha^{g(m)}$ 和 $\alpha^{kg(r)+k's} = (\alpha^k)^{g(r)} r^s$.
2. 如果第一步计算出的两个值相等, 那么他就认为这个签名是有效的.

对于这个签名方案安全性的分析参见原始文献 [ElGamal, 1985], pp.470–471. 非常关键的一点是: 对于不同的消息应当选择不同的随机数 k', 否则利用两个明文及其对应的签名就能通过求解由 (1.1) 形成的线性方程组, 来获取 k' 以及 Kevin 的私钥 k.

这个方案的一个主要缺陷是传输数据长度的扩展 —— 被签消息的长度是原消息长度的三倍. 这个被扩展的数据可以利用一个 hash 函数来压缩. 在实际应用中, 一次会话中被传送的数据由若干 $m_1, m_2, \cdots, m_n$ 组成. 而 hash 函数就是函数

$$h : \mathcal{M}^{(\mathbb{N})} \to \mathcal{H},$$

这里 $\mathcal{M}^{(\mathbb{N})}$ 表示由 $\mathcal{M}$ 中元素构成的有限序列集合，$\mathcal{H}$ 是一个有限集合. 我们可以对 $h(m_1, m_2, \cdots, m_n)$ 进行签名而不是对每一个 m_i 分别签名. 为了防止伪造签名，h 必须是一个单向函数.

数字签名标准

1994 年，美国国家标准技术局 (NIST)公布了一个数字签名的标准 (DSS)，美国国家机构必须执行这个签名的标准 (参见 [NIST, 1994]). 除了描述特定 hash 函数的使用以外，DSS 给出了一个数字签名算法 (DSA). (在更新后的版本中也允许使用 RSA 签名算法，参见 [NIST, 1998].) 通常的设置如下：

1. p 是一个素数并且满足 $2^{L-1} < p < 2^L$，其中
$$L \in \{512, 576, 640, 704, 768, 832, 896, 960, 1024\}.$$
2. q 是 $p-1$ 的一个素因子，并且满足 $2^{159} < q < 2^{160}$.
3. $\alpha \in \mathbb{F}_p$ 是群 $\mathbb{F}_p^\times$ 中唯一阶为 q 的子群的生成元. 该签名算法是基于群 $\langle\alpha\rangle$ 中的离散对数问题.
4. 函数
$$g : \mathbb{F}_p^\times = \{1, \cdots, p-1\} \to \{0, \cdots, q-1\}$$
表示模 q 约化：对于 $\alpha \in \{1, \cdots, p-1\}$，
$$g(\alpha) \equiv \alpha \pmod q.$$
5. $h : \mathcal{M}^{(\mathbb{N})} \to \mathbb{Z}$ 是由安全 hash 函数标准 (SHS) 来确定的 hash 函数，该标准可参见 [NIST, 1995]. Kevin 的私钥是整数 k，$0 < k < q$，其公钥是 α^k. 假设 m 是待签消息.

签名

1. Kevin 随机选择一个整数 k'，$0 < k' < q$，并计算 $r = \alpha^{k'}$ 与 $g(r)$.
2. Kevin 求解同余方程
$$h(m) \equiv -kg(r) + k's \pmod q \tag{1.2}$$
的解 s，$0 < s < q$.
3. 签名就是数对 $(g(r), s) \in \mathbb{Z}_q \times \mathbb{Z}_q$.

验证签名

1. Laura 求同余方程 $\omega s \equiv 1 \pmod q$ 的解 ω, $0 < \omega < q$. 计算

$$u_1 \equiv h(m)\omega \pmod q$$
$$u_2 \equiv g(r)\omega \pmod q,$$

其中 $0 \leqslant u_1, u_2 < q$, 以及 $v = g(\alpha^{u_1}(\alpha^k)^{u_2})$.

2. 如果 $v = g(r)$, 则 Laura 就认为该签名有效.

下面验证 Laura 能接受一个合法的签名. 由 (1.2) 可知

$$\alpha^{u_1}(\alpha^k)^{u_2} = \alpha^{h(m)\omega + kg(r)\omega} = \alpha^{k' s\omega} = \alpha^{k'}.$$

因此

$$v = g(\alpha^{u_1}(\alpha^k)^{u_2}) = g(r).$$

对于 $\mathbb{F}_p^\times$ 中元素进行模 q 约化的目的是将签名长度由 $2L$ 比特压缩为 320 比特. 实际上它可以是任意一个映射 $g: \mathbb{F}_p^\times \to \{0, \cdots, q-1\}$, 因为这与 $\mathbb{F}_p$ 的乘法结构是不相容的.

这个签名方案可以直接地推广到任意有限循环群 $G = \langle \alpha \rangle$, 并且可以看出 DSA 与 ElGamal 算法在某种意义下是类似的：签名过程完全一样，而验证过程只是做了一点修改，同时这里知道的是 $g(r)$ 而不是 r.

1.5 标 准

由于公钥密码学的应用范围越来越广，因此不同的国家和国际组织正致力于算法及其参数的标准化工作. 下面我们简要介绍一些可以公开获取的文件.

电气和电子工程师协会正准备对公钥密码学, 包括各种基本的加密算法、签名方案以及秘密共享协议制定一个综合的标准 [IEEE, 1998]. 美国联邦标准局为金融行业发布了一系列的标准. 像 Diffie-Hellman 的密钥交换协议一样，[ANSI, 1998a] 详细说明了基于有限域上离散对数问题的密钥共享协议. 相关内容可进一步参阅文献 [ANSI, 1999] 和 [ANSI, 1998b]. [ANSI, 1999] 涵盖了基于椭圆曲线的密钥交换方案，而 [ANSI, 1998b] 详细说明了椭圆曲线上类似于 DSA 的算法 ——ECDSA.

我们在 1.4 节已经说明美国政府规定电子签名时 DSA 和 RSA 的使用. 欧盟政策更为灵活. 他们主要关注电子签名的合法性，也更倾向于确保认证服务，而这种认证服务是将一个人与其签名紧密联系起来所必需的，但欧盟并没有规定具体使

用那些技术:“现在有许多有关利用公钥密码实现数字签名的研究与讨论，欧盟内部的指导原则应当在技术上是中立的，不应该是只关注到现有的几种签名技术. 由于许多不同的认证技术正不断发展，指导原则必须具有足够的包容度，能够涵盖所有的‘电子签名’. 这里电子签名不仅包括基于公钥密码的数字签名，也包括基于其他认证方式的数字签名.” ([Commission of the European Communities, 1998], p.3) 但是欧盟希望能够有国际标准出现并鼓励工业界采用这些标准. 关于欧洲不同的国家采取的法律措施参见 [Commission of the European Communities, 1998].

为给出电子签名的一个国际性法律构架，联合国也采用这种并不只是将精力集中到一些特殊技术上的策略，参见 [UNCITRAL, 1998a] 和 [UNCITRAL, 1998b].

第 2 章　椭圆曲线上的群运算

由于椭圆曲线上可以建立起能够有效计算的群运算法则，因此它适合于建立第 1 章中提及的密码体制，这一点最早由 Koblitz 和 Miller 分别在 [Koblitz, 1987] 和 [Miller, 1986] 中提出. 椭圆曲线密码最吸引人之处在于其能够用较短的密钥长度来达到与基于有限域的密码体制相当的安全性要求，从而能够以较快的速度完成加密和解密运算. 本章的主要目的是证明其群运算法则.

在给出一些必要的定义之后，我们将利用直线及其与曲线的交点来直观解释椭圆曲线上的运算规则，并通过一些初等的计算来得到适合计算机实现的具体代数表达式. 这样的运算规则符合群的公理体系，但是其中结合律的证明是较为困难的. 对此有以下几种证明途径：

一种明显的方式是在给定曲线上的点加公式之后，进行直接的计算. 但是由于随着点相对位置的不同，点加公式也可能不同，这样就需要分多种情况加以讨论. 更糟糕的是，这样的证明方法并不能揭示出内在的代数和几何结构. 因此这样的处理方式不仅非常繁琐，而且没有直观意义. 也许正是由于这一点，许多作者望而却步. 据我所知没有哪本书是采用直接计算来完成结合律的证明的.

许多作者考虑复数域上的椭圆曲线，并利用复数域的解析结构来揭示其特殊性质，可参阅 [Koblitz, 1993], [Lang, 1978] 或 [Lang, 1987]. 但是对应用而言，我们主要感兴趣的是有限域上的椭圆曲线. 此时就不能使用解析的证明方法. 为此在本书中，我们采用纯代数的方法，该方法对任意域都是适用的. 不过如果将得到的代数结论与相应的解析结果联系起来将更具启发性. 为此建议读者对以上提及的参考书目详细的阅读.

在一般理论作了一些改进后, Fulton 在他的书 ([Fulton, 1969], p.125) 中给出了一个基于代数曲线的优美的几何证明. 同样的证明也可参见 [Husemöller, 1987] 中的第 3 章. 另外一种处理方式是使用 Riemann-Roch 定理，感兴趣的读者可在 [Fulton, 1969] 的第 8 章中找到该定理. 对于代数几何方面的专家来说，这样的处理方式是非常理想的. 这方面经典的参考书是 [Silverman, 1986] 和 [Silverman, 1994]. 不过从代数几何的观点上看，椭圆曲线是比较“简单”的，在不具备大量抽象代数几何知识的情况下也是可以理解的.

本章中，我们采用 Charlap 和 Robbin 给出的初等证明方法 [Charlap and Robbins, 1988]. 一方面，我们介绍代数曲线理论中的一些基本概念，从而使读者对此有

一个初步的了解. 另一方面，我们只讨论椭圆曲线上的相关结论. 这样处理可以使许多结果通过直接计算或是简单讨论就能得以证明，从而使表述更加具体和基础. 与 Charlap 和 Robbins 不同的是在涉及无穷远点 $\mathcal{O}$ 时，我们统一使用射影坐标的观点，以使 $\mathcal{O}$ 的引入更加自然. 同时我们给出的关于结合律的证明是具有一般性的，其适用于任意特征的域，其中也包括密码学中常用的特征等于 2 的情况.

要注意本章中 K 总是表示代数闭域.

2.1 仿射平面曲线

在本节中我们重点介绍有关仿射曲线的基本定义和基本概念，为后面几节进一步具体讨论椭圆曲线奠定基础.

定义2.1 集合 $K \times K$ 被称为 K 上的仿射平面，记为 $A^2(K)$.

定义2.2 仿射平面上不可约多项式 $C \in K[X,Y]$ 的全部零点构成的集合，即

$$\{(x,y) \in A^2(K) : C(x,y) = 0\},$$

被称为 K 上的仿射平面曲线.

例 当 $K = \mathbb{R}$ 时，曲线 $D = Y^2 - (X^3 + X^2)$ 和 $E = Y^2 - (X^3 - X)$ 如图 2.1 所示.

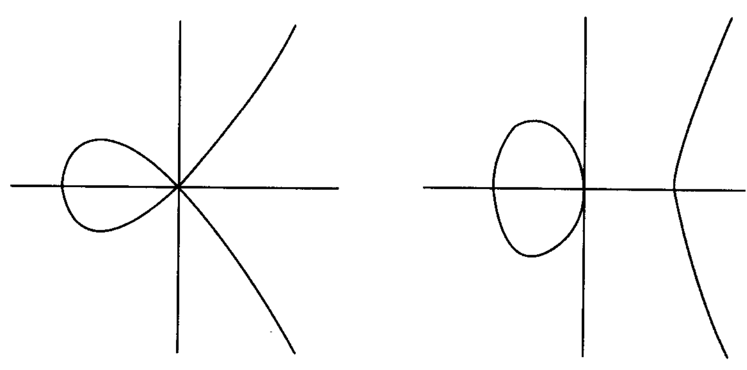


图 2.1 曲线 $Y^2 = X^3 + X^2$ 和 $Y^2 = X^3 - X$

由于 K 是代数闭域，因此任意一条仿射平面曲线都包含无穷多个点：对任意的 $x \in K$，在 K 中方程 $C(x,Y) = 0$ 至少有一个零点 y，即得到曲线上的点 $P = (x,y)$. 而代数闭域有无穷多个元素，因此仿射平面曲线上也有无穷多个点. 为简便起见，

我们用定义曲线的多项式 C 来表示该曲线，并称其为"由 C 所定义的曲线"、"曲线方程为 C"或简称为"曲线 C".

定义2.3　设 C 是一条曲线，$P=(x,y)$ 是曲线 C 上的点. 如果

$$\frac{\partial C}{\partial X}(x,y)=\frac{\partial C}{\partial Y}(x,y)=0,$$

则称 P 在 C 上是奇异的. 如果曲线上至少有一个奇异点，则称该曲线为奇异曲线.

例　由于

$$\frac{\partial D}{\partial X}(0,0)=-(3X^2+2X)\mid_{X=0}=0,\quad \frac{\partial D}{\partial Y}=2Y\mid_{Y=0}=0,$$

因此原点是曲线 D 上的奇异点. 但是由于

$$\frac{\partial E}{\partial X}(0,0)=(-3X^2+1)\mid_{X=0}=1\neq 0,$$

因此原点不是曲线 E 上的奇异点. 从几何的角度上看，点的非奇异性意味着该点处有唯一的切线. 例如曲线 E 在原点处的切线就是垂直线 (即 Y 轴). 而从图 2.1 可以看到，曲线 D 在奇异点 $(0,0)$ 处有两条不同的切线：$Y=X$ 和 $Y=-X$. 此时原点被称为结点. 另一种可能的情况是所谓的尖点，即其有一条多重切线. 我们将在 2.9 节继续讨论切线问题并给出严格的定义.

我们感兴趣的是定义在曲线上的多项式函数. 显然如果两个多项式 f,g 只相差 C 的一个倍数，即 $C\mid f-g$，则在曲线 C 上 f,g 可以看成是相同的. 实际上，反向的结论也是成立的. 我们将在 2.2 节中针对椭圆曲线这一具体情形给出相应的证明. 这样就得到以下的定义：

定义2.4　称 $K[C]:=K[X,Y]/(C)$ 为曲线 C 的坐标环.

为简便起见，我们仍然用 X,Y 分别表示 $K[C]$ 中 X,Y 所在的剩余类，其意义在上下文中是明确的. 由于 C 是不可约多项式，因此 $K[C]$ 是一个整环.

定义2.5　$K[C]$ 的分式域被称为是 C 上的有理函数域，记为 $K(C)$.

对于曲线上给定的点，我们可以通过代入其 X 坐标和 Y 坐标来计算坐标环中某一多项式在该点的值. 但是对于有理函数而言，这样的做法有时是行不通的，因为其分母可能是零. 要注意的是虽然 $K[X,Y]$ 是唯一分解整环，但坐标环 $K[C]$ 却未必是唯一分解整环.

定义2.6 设 P 是曲线 C 上的点. 如果对于有理函数 $r \in K(C)$, 存在 $f, g \in K[C]$, 使得 $r = \dfrac{f}{g}$ 且 $g(P) \neq 0$, 则称 r 在点 P 处是正则的, 或称在点 P 处是可定义的. 此时 r 在 P 点的值就是 $r(P) = \dfrac{f(P)}{g(P)}$. 称在 P 点正则处的全体有理函数所组成的环为 C 在 P 点处的局部环, 记为 $\mathcal{O}_P(C)$. 通常当 r 在 P 点处不正则时, 记为 $r(P) = \infty$.

要注意的是以上关于正则有理函数在某个点处的值的定义是有意义的, 即其与该函数写成两个多项式的商的表示形式无关: 设

$$r = \frac{f_1}{g_1} = \frac{f_2}{g_2},$$

其中 $f_1, g_1, f_2, g_2 \in K[C]$ 且 $g_1(P), g_2(P) \neq 0$, 则在 $K[C]$ 中有 $f_1g_2 = f_2g_1$, 即存在多项式 $h \in K[X, Y]$ 满足 $f_1g_2 - f_2g_1 = hC$, 因此

$$f_1(P)g_2(P) - f_2(P)g_1(P) = h(P)C(P) = h(P) \cdot 0 = 0,$$

即 $\dfrac{f_1(P)}{g_1(P)} = \dfrac{f_2(P)}{g_2(P)}$.

容易验证 $\mathcal{O}_P(C)$ 的确是一个环, 而且是一个局部环: 其单位 (即可逆元)的全体为

$$\mathcal{O}_P(C)^{\times} = \left\{ \frac{f}{g} : f(P), g(P) \neq 0 \right\},$$

其唯一的极大理想是

$$\mathfrak{m}_P(C) = \left\{ \frac{f}{g} : g(P) \neq 0, f(P) = 0 \right\}.$$

例 设 $E : Y^2 = X^3 - X$, 其图像如图 2.1 的右侧所示. 考虑有理函数 $r = \dfrac{X}{Y}$. 当 $P = (0, 0)$ 时,

$$X(P) = Y(P) = 0,$$

即此时分子、分母全为零. 但是我们可以取 r 的另一种表示形式:

$$r = \frac{X}{Y} = \frac{XY}{Y^2} = \frac{XY}{X^3 - X} = \frac{Y}{X^2 - 1}.$$

此时 $Y(P) = 0, (X^2 - 1)(P) = -1 \neq 0$, 因此 r 在 P 点处是正则的, 且 $r(P) = \dfrac{0}{-1} = 0$.

设 $s=\frac{1}{r}=\frac{Y}{X}$, 则 s 在 P 点处就不是正则的. 否则 $s(P)\in K$, 从而就得出

$$1=1(P)=(rs)(P)=r(P)s(P)=0\ s(P)=0,$$

这是矛盾的.

2.2 仿射椭圆曲线

在本节中将介绍学习的主要对象 —— 椭圆曲线. 我们将仔细考察其坐标环和有理函数域, 此时它们的形式是比较特殊的.

定义2.7 称形如

$$E: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6,\quad a_1,a_3,a_2,a_4,a_6\in K$$

的方程为 K 上的仿射Weierstrass方程. 记

$$\begin{aligned}
b_2&=a_1^2+4a_2,\\
b_4&=2a_4+a_1a_3,\\
b_6&=a_3^2+4a_6,\\
b_8&=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,\\
c_4&=b_2^2-24b_4,\\
\Delta&=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6,\\
j&=\frac{c_4^3}{\Delta},\quad 当\Delta\neq 0时,
\end{aligned}$$

其中 Δ 被称为 E 的判别式, j 被称为 j 不变量. 由非奇异Weierstrass 方程定义的曲线被称为椭圆曲线.

b_2,b_4,b_6,b_8,c_4 只是被用来简化 Δ 和 j 的定义. 在 2.4 节中我们将会看到 Δ 确定了 Weierstrass 方程是否奇异. 在本书中, 我们并不过多涉及 j 不变量, 只是在 2.3 节讨论标准形式以及 3.11 节中会用到 j 不变量. 为简便起见, 我们对椭圆曲线和定义该椭圆曲线的方程或多项式并不加以区分, 并都用符号 E 来表示. 当我们称 E 是一个多项式时, 就是指 $E=Y^2+a_1XY+a_3Y-(X^3+a_2X^2+a_4X+a_6)$.

首先我们说明以上关于椭圆曲线的定义是符合 2.1 节中曲线的定义的, 即 Weierstrass 方程是不可约的.

在 $K(X)$ 中, 函数 $\frac{f}{g}$ 的次数为

$$\deg \frac{f}{g} = \deg f - \deg g, \quad f, g \in K[X].$$

因此对于 $r, s \in K(X)$, 有

$$\begin{aligned} \deg(rs) &= \deg r + \deg s, \\ \deg \frac{1}{r} &= -\deg r, \\ \deg(r+s) &\leqslant \max\{\deg r, \deg s\}, \quad \text{当 } \deg r \neq \deg s \text{ 时等号成立}. \end{aligned}$$

由于对于 Y 而言 E 是首一多项式, 且 $K[X]$ 是唯一分解整环, 因此 E 在 $K[X,Y]$ 中不可约的充要条件是其在 $K(X)[Y]$ 中不可约. 假设 E 是可约的, 则其可以表示为 $(Y+r)(Y+s)$ 的形式, 其中 $r, s \in K(X)$. 比较 Y 的系数可得

$$r + s = a_1X + a_3, \quad rs = -(X^3 + a_2X^2 + a_4X + a_6),$$

因此 $\deg(r+s) \leqslant 1$ 且 $\deg(rs) = \deg r + \deg s = 3$ 是奇数, 所以 $\deg r \neq \deg s$. 由此可得

$$1 \geqslant \deg(r+s) = \max\{\deg r, \deg s\} \geqslant \frac{1}{2}(\deg r + \deg s) = \frac{3}{2},$$

这是矛盾的.

由上可知 E 是不可约的, 因此由 2.1 节知可以定义 $K[E] = K[X,Y]/(E)$ 及其分式域 $K(E)$. $K[E]$ 中的每个元素可看作椭圆曲线 E 上点的一个多项式函数. 同时 $K[E]$ 中两个不同的元素作为曲线上的多项式函数也是不同的. 这点并不是显而易见的. 我们现在来证明这一结论. 显然只要证明: 如果 $f \in K[E]$ 作为 E 上的函数恒等于零, 即对任意的点 $P \in E$ 都有 $f(P) = 0$, 则 f 必定是 $K[E]$ 中的零元. 这一结论对任意的曲线都是成立的, 但当 E 是椭圆曲线时, 证明是比较简单的.

为此我们从另一个角度来考察有理函数域 $K(E)$. 显然 $K[X]$ 是 $K[E]$ 的子环, 因此 $K(X)$ 就是 $K(E)$ 的子域. 对 $K(X)$ 添加变量 Y 并模 E 后可得 $L := K(X)[Y]/(E)$. 由于 E 在 $K(X)$ 上是不可约的, 因此 L 是一个域. 由于 $K[E] \subseteq L \subseteq K(E)$, 而 $K(E)$ 是 $K[E]$ 的分式域, 即其是包含 $K[E]$ 的最小的域, 所以有 $L = K(E)$. 由此可知 $K(E)$ 是 $K(X)$ 的二次扩域, 因此 $K(E)$ 的唯一非平凡 $K(X)$ 自同构将 Y 作用到 E 在 $K(X)$ 上的另一个根 $\overline{Y} = -Y - a_1X - a_3$. 用 $\overline{f}$ 表示 f 的共轭, 即用 $\overline{Y}$ 代替每个 Y. 同样地, 对于点 $P = (x, y) \in E$, 定义其共轭 $\overline{P} = (\overline{X}, \overline{Y})(P) = (x, -y - a_1x - a_3)$, 因此有 $\overline{f}(P) = f(\overline{P})$.

定义2.8　对于域的扩张 $K(E)/K(X)$, 定义 $K(E)$ 上的范函数和迹函数分别为

$$\mathrm{N}: \quad K(E) \to K(X), \quad f \mapsto f\overline{f},$$
$$\mathrm{Tr}: \quad K(E) \to K(X), \quad f \mapsto f + \overline{f}.$$

例　对于坐标函数 X, Y, 有

$$\mathrm{N}(X) = X^2, \qquad \mathrm{Tr}(X) = 2X,$$
$$\mathrm{N}(Y) = -(X^3 + a_2X^2 + a_4X + a_6), \qquad \mathrm{Tr}(Y) = -(a_1X + a_3).$$

更一般地, 如果 $f = v + Yw \in K(E)$, 其中 $v, w \in K(X)$, 则 $\overline{f} = v + \overline{Y}w$. 由此可得

$$\mathrm{N}(f) = v^2 + \mathrm{Tr}(Y)vw + \mathrm{N}(Y)w^2, \qquad \mathrm{Tr}(f) = 2v + \mathrm{Tr}(Y)w.$$

由于范函数能够将二元多项式约化为简单的一元多项式, 因此在本章中范函数将是一个非常有用的工具. 下面就利用范函数来证明 $K[E]$ 是由 E 上多项式函数构成的环: 设 $f \in K(E)$ 是 E 上的零函数, 则 $\mathrm{N}(f)$ 在 E 上也恒等于零. 由于 $\mathrm{N}(f) \in K(X)$ 且对于任意的 $x \in K$, 其都是 E 上某点的 X 坐标, 因此 $\mathrm{N}(f) = 0$, 从而 $f = 0$.

2.3　变量变换与标准形式

虽然我们直接讨论椭圆曲线的方法并不需要非常多的理论知识, 但这样处理的缺点是需要大量的计算. 为减少所需的计算, 考虑对椭圆曲线方程加以变换, 使得某些系数 a_i 等于 0. 当然我们要求这样的变换并不会改变曲线的“特性”.

定义2.9　对于由Weierstrass 方程确定的两条曲线

$$E: \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$
$$E': \quad Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',$$

如果 E 可以通过以下形式的变量变换得到 E'

$$\psi: \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} u^2X + r \\ u^3Y + u^2sX + t \end{pmatrix} = \begin{pmatrix} u^2 & 0 \\ u^2s & u^3 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix},$$

其中 $u \in K^{\times}, r, s, t \in K$(并对最终得到的等式两边约去 u^6), 则称 E 和 E' 是同构的, 而变换 ψ 被称为是容许的变量变换.

例 坐标函数的共轭

$$(X,Y) \mapsto (\overline{X},\overline{Y}) = (X, -Y - a_1X - a_3)$$

就是一个容许的变量代换，其中 $u=-1, r=0, s=-a_1, t=-a_3$，而且其是一个对合，即其逆变换就是它自己.

实际上以上的定义是一个定理：在仿射平面的代数子簇所在的范畴中，能够保持 Weierstrass 方程不变的唯一同构必定具有上述变量变换的形式. 由于我们并不打算详细学习代数几何的相关内容，对以上的定义做一些看似合理的说明就足够了.

首先我们说明上面的定义是有意义的，即 Weierstrass 方程之间的同构关系是一个等价关系. 显然令 $u=1, r=s=t=0$，则可知恒等变换

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix}$$

是一个容许的变量变换，所以其满足自反性. ψ 的逆变换是

$$\psi^{-1}: \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} u^{-2} & 0 \\ -u^{-3}s & u^{-3} \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} - \begin{pmatrix} u^{-2}r \\ u^{-3}(t-rs) \end{pmatrix}.$$

显然其也是容许的变量变换，因此同构关系是对称的. 通过一些简单的计算也可以证明同构关系也满足传递性. 具体的证明留给读者.

另一方面，曲线被定义成点集，而容许的变量变换 ψ 对应着互逆的双射

$$\begin{aligned} \varphi &: E \to E',(x,y) \mapsto (u^{-2}(x-r), u^{-3}(y-sx-t+rs)), \\ \varphi' &: E' \to E,(x,y) \mapsto (u^2x+r, u^3y+u^2sx+t), \end{aligned}$$

且有 $\varphi' \circ \varphi = \mathrm{id}\,|_E$，$\varphi \circ \varphi' = \mathrm{id}\,|_{E'}$，因此 “同构” 的概念是恰当的.

假如要使用仿射坐标变换，那么就必须确保存在仿射逆变换. 在这一要求下，容易说明容许的变量变换是唯一可能的选择. 设

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

将 E 变换为 $E(\alpha X+\beta Y+r, \gamma X+\delta Y+t)$，而 $E(\alpha X+\beta Y+r, \gamma X+\delta Y+t)$ 与 E' 相差一个可逆因子. 由于在 E 中 X 的次数等于 3，而 E' 中 Y 的次数等于 2，因此有 $\beta=0$. 同时由于 X^3, Y^2 在所得方程中的系数必须相等且不等于 0，即 $\alpha^3=\delta^2\neq 0$，

因此对于某个 $u \in K^{\times}$ 有 $\alpha = u^2, \delta = u^3$(注意 K 是一个代数闭域). 最后令 $s = \dfrac{\gamma}{u^2}$ 即可.

将坐标变换代入 E 的方程. 通过与 E' 的方程进行系数之间的比较，可知 E' 的诸系数 a'_i 以及定义 2.7 中所给出的各个参数与 E 中相应参数之间的关系如表 2.1 所示. 注意同构椭圆曲线的 j 不变量是相同的，这也是称其是"不变量"的原因. 事实上，不难证明对于代数闭域 K，如果 K 上两条曲线具有相同的 j 不变量，则它们必定是同构的. (参见 [Silverman, 1986], 命题 1.4(b) 和 A.1.2(b).)

表 2.1　同构椭圆曲线的系数

$$
\begin{aligned}
a'_1 &= u^{-1}(a_1 + 2s)\\
a'_3 &= u^{-3}(a_3 + ra_1 + 2t)\\
a'_2 &= u^{-2}(a_2 - sa_1 + 3r - s^2)\\
a'_4 &= u^{-4}(a_4 + 2ra_2 - (rs+t)a_1 - sa_3 + 3r^2 - 2st)\\
a'_6 &= u^{-6}(a_6 + r^2a_2 + ra_4 - rta_1 - ta_3 + r^3 - t^2)\\
b'_2 &= u^{-2}(b_2 + 12r)\\
b'_4 &= u^{-4}(b_4 + rb_2 + 6r^2)\\
b'_6 &= u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3)\\
b'_8 &= u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)\\
c'_4 &= u^{-4}c_4\\
\Delta' &= u^{-12}\Delta\\
j' &= j
\end{aligned}
$$

显然容许的变量变换 ψ 可以扩张为 $K[E], K[E']$ 之间的同构，进而也可扩展为 $K(E), K(E')$ 之间的同构. 对此我们仍然用 ψ 来表示. 由于 ψ 保持多项式及有理函数的值，因此对于任意的 $P \in E$，ψ 也可扩张为局部环 $\mathcal{O}_P(E)$ 和 $\mathcal{O}_{\varphi(P)}(E')$ 之间的同构.

可以看到 $\psi(K(X)) \subseteq K(X)$ 且 $\psi^{-1}(K(X)) \subseteq K(X)$，因此 ψ 也是 $K(X)$ 的自同构. 由此可以证明 ψ 保持共轭性，即对于 $f \subsetneq K(E)$，有 $\psi(\overline{f}) = \overline{\psi(f)}$. 设 ι 是 $K(E)$ 上的共轭映射，显然 $\iota' := \psi \circ \iota \circ \psi^{-1}$ 是 $K(E')$ 上的自同构，其固定域为 $K(X)$：

$$
\begin{aligned}
&(\psi \circ \iota \circ \psi^{-1})(f) = f\\
\Longleftrightarrow\, &\iota(\psi^{-1}(f)) = \psi^{-1}(f)\\
\Longleftrightarrow\, &\psi^{-1}(f) \in K(X) \qquad (\text{由于}\iota\text{的固定域为}K(X))
\end{aligned}
$$

$$\Longleftrightarrow f \in \psi(K(X)) = K(X).$$

因此 ι' 是 $K(E')$ 上的共轭. 由此可知

$$\overline{\psi(f)} = (\iota' \circ \psi)(f) = (\psi \circ \iota)(f) = \psi(\overline{f}),$$

因此也就有 $\mathrm{N}(\psi(f)) = \psi(\mathrm{N}(f))$, $\mathrm{Tr}(\psi(f)) = \psi(\mathrm{Tr}(f))$.

由以上的讨论可知, 无论是考虑有理函数还是考虑由局部环 $\mathcal{O}_P(E)$ 所反映的 E 的 "局部" 性质, 或者是考虑共轭、迹以及范, 都只要考察 E 所在的同构类即可. 本节余下的部分将对每个椭圆曲线, 给出具有 "简单" 形式的同构表示.

当 $\mathrm{char}(K) \neq 2$ 时, 首先对 Weierstrass 方程的左边进行配方, 相应的容许变量变换 $(X, Y) \mapsto \left(X, Y - \dfrac{1}{2}(a_1X + a_3)\right)$ 将 E 变换为

$$E' : Y^2 = X^3 + a_1'X^2 + a_4'X + a_6'.$$

进一步地, 如果又有 $\mathrm{char}(K) \neq 3$, 则由 $(X, Y) \mapsto \left(X - \dfrac{1}{3}a_2', Y\right)$ 就可以消去右式中 X 的平方项, 得到

$$E'' : Y^2 = X^3 + a_4''X + a_6''.$$

当 $\mathrm{char}(K) = 3$ 时, 我们希望消去方程 E' 中的某一项. 如果 $a_2' = 0$(即当 $\Delta \neq 0$ 时, 有 $j' = \dfrac{a_2'^6}{\Delta} = 0$), 则此时 E' 已经是所希望的标准形式. 否则由 $(X, Y) \mapsto \left(X + \dfrac{a_4'}{a_2'}, Y\right)$ 可得

$$E'' : Y^2 = X^3 + a_2''X^2 + a_6''.$$

当 $\mathrm{char}(K) = 2$ 时, 我们也分两种情况加以讨论. 当 $a_1 = 0$ 时, 即当 $\Delta \neq 0$ 时有 $j = \dfrac{a_1^{12}}{\Delta} = 0$, 由 $(X, Y) \mapsto (X + a_2, Y)$ 就可以消去 X 的平方项. 否则, 利用容许的变量变换

$$(X, Y) \mapsto \left(a_1^2X + \frac{a_3}{a_1}, a_1^3Y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right),$$

可得如下形式的曲线

$$E'' : Y^2 + XY = X^3 + a_2''X^2 + a_6''.$$

表 2.2 给出了当 $\Delta \neq 0$ 时的各种标准形式 (此时 j 不变量是有意义的). 我们已经看到, 对于适当的 a_1, a_2, 曲线的 Δ 可能为零.

表 2.2 椭圆曲线的标准形式

标准形式	Δ	j
$\mathrm{char}(K)\neq 2,3$		
$Y^2=X^3+a_4X+a_6$	$-16(4a_4^3+27a_6^2)$	$1728\dfrac{4a_4^3}{4a_4^3+27a_6^2}$
$\mathrm{char}(K)=3, j\neq 0$		
$Y^2=X^3+a_2X^2+a_6$	$-a_2^3a_6$	$-\dfrac{a_2^3}{a_6}$
$\mathrm{char}(K)=3, j=0$		
$Y^2=X^3+a_4X+a_6$	$-a_4^3$	0
$\mathrm{char}(K)=2, j\neq 0$		
$Y^2+XY=X^3+a_2X^2+a_6$	a_6	$\dfrac{1}{a_6}$
$\mathrm{char}(K)=2, j=0$		
$Y^2+a_3Y=X^3+a_4X+a_6$	a_3^4	0

2.4 奇 异 性

对于由 Weierstrass 方程定义的曲线，其是否奇异可以用一个简单的方法加以判断.

定理2.10 *由Weierstrass方程定义的曲线奇异的充要条件是其判别式等于 0.*

证明 由表 2.1 可以看到，容许的变量变换对于判别式的影响只是相差一个非零因子，而且由于仿射变换能够保持曲线的奇异性不变，因此只需对表 2.2 中的标准形式证明该定理即可.

当 $\mathrm{char}\,K\neq 2$ 时，此时可假定曲线 E 的形式是 $Y^2=X^3+a_2X^2+a_4X+a_6$. 其判别式 Δ 等于函数 $f=X^3+a_2X^2+a_4X+a_6$ 判别式的 16 倍. 由此可知 $\Delta=0$ 的充要条件是 f 有重根. 由于 $P=(x,y)$ 是 E 上的奇异点的充要条件是 $E(x,y)=2y=f'(x)=0$，即 $y=0, f(x)=f'(x)=0$，因此定理成立.

当 $\mathrm{char}(K)=2$ 时，我们分以下两种情况讨论:

1. 当 $E=Y^2+XY+X^3+a_2X^2+a_6, \Delta=a_6$ 时，有

$$\frac{\partial E}{\partial X}(X,Y)=Y+X^2,$$
$$\frac{\partial E}{\partial Y}(X,Y)=X.$$

因此 $P=(x,y)$ 是 E 上的奇异点的充要条件是 $x=0$, $y+x^2=0$, $E(x,y)=0$, 也就是 $x=y=E(0,0)=0$, 所以有 $a_6=0$.

2. 当 $E=Y^2+a_3Y+X^3+a_4X+a_6, \Delta=a_3^4$ 时, 有

$$\frac{\partial E}{\partial X}(X,Y)=X^2+a_4,$$
$$\frac{\partial E}{\partial Y}(X,Y)=a_3.$$

显然只有当 $a_3=0$ 时, E 才有奇异点. 而此时 $(\sqrt{a_4},\sqrt{a_6})$ 就是一个奇异点. □

2.5 局部环 $\mathcal{O}_P(E)$

在定义 2.6 中我们已经指出 $\mathcal{O}_P(E)$ 是一个局部环, 即其有唯一的极大理想 $\mathfrak{m}_P$. 实际上, $\mathcal{O}_P(E)$ 还是一个离散赋值环:

定理2.11 对于椭圆曲线 E 以及 E 上的点 P, 环 $\mathcal{O}_P(E)$ 是一个离散赋值环, 即存在 $u\in\mathfrak{m}_P(E)$, 使得任意的 $s\in\mathcal{O}_P(E)\backslash\{0\}$, 都可以表示为

$$s=u^dr,$$

其中 d 是一个非负整数, 而 $r\in\mathcal{O}_P(E)^\times$.

u 被称为是 $\mathcal{O}_P(E)$ 的一致化参数. 可以证明 d 与一致化参数 u 的选取是无关的: 实际上 u 是 $\mathfrak{m}_P(E)$ 的生成元, 而 d 是满足 $s\in\mathfrak{m}_P(E)^d$ 且 $s\notin\mathfrak{m}_P(E)^{d+1}$ 的唯一非负整数.

定理 2.11 实际上反映了任意曲线上非奇异点的特性. 在 2.9 节中我们将说明在给定点处的一条直线, 如果其不是曲线在该点处的切线的话, 那么该直线就是该点处局部环的一个一致化参数. 而在这里, 我们通过对每个点取特定的一致化参数来证明定理 2.11. 为此我们首先给出 2 阶点的概念, 其在证明过程中需要单独处理.

定义2.12 如果点 $P=(x,y)$ 满足 $P=\overline{P}$, 即

$$Y(P)=y=-y-a_1x-a_3=\overline{Y}(P),$$

则称 P 为 2 阶点.

2 阶点实际上就是 2.11 节中定义的群运算中阶等于 2 的点. 首先考察 2 阶点的存在性. 由于椭圆曲线的同构是保持共轭性的 (参见 2.3 节), 因此只需要考虑表 2.2 中标准形式的椭圆曲线即可.

- $\operatorname{char} K \neq 2$; $Y^2 = X^3 + a_2X^2 + a_4X + a_6$
  当$y = -y = 0$ 时 (x, y) 为 2 阶点. 这样恰好有 3 个 2 阶点 $(x, 0)$, 其中 x 是 $X^3 + a_2X^2 + a_4X + a_6$(不相同) 的根.
- $\operatorname{char} K = 2$, $j \neq 0$; $Y^2 + XY = X^3 + a_2X^2 + a_6$, $a_6 \neq 0$
  当 $0 = 2y = x$ 时 (x, y) 为 2 阶点, 因此 2 阶点只有一个, 即 $(0, \sqrt{a_6})$.
- $\operatorname{char} K = 2$, $j = 0$; $Y^2 + a_3Y = X^3 + a_4X + a_6$, $a_3 \neq 0$
  如果 (x, y) 为 2 阶点, 则 $0 = 2y = a_3$, 因此此时 2 阶点并不存在.

定理 2.11 的证明　首先要注意 $\mathfrak{m}_P$ 是由以 P 为零点的函数构成的理想, 而 $\mathcal{O}_P^\times$ 是由在 P 点处正则且不等于零的函数所构成的集合.

设 $s \in \mathcal{O}_P(E)$, 则 $s = \dfrac{f}{g}$, 其中 $f, g \in K[E]$ 且 $g(P) \neq 0$, 因此 g 是单位, 从而只需对多项式函数 f 完成定理的证明即可. 如果 $f(P) \neq 0$, 则 f 也是单位而 $d = 0$, 所以在下面的证明中我们均假设 $f(P) = 0$.

- 如果 $P = (x, y)$ 不是 2 阶点, 则 $u = X - x$ 就是一个一致化参数.
  记 $f = v + Yw$, 其中 $v, w \in K[X]$, 然后不断地同时从 v 和 w 中分解出因子 $X - x$, 直至 v 和 w 中至少有一个不再被 $X - x$ 整除. 此时有

$$f = (X - x)^{d_1}(v_1(X) + Yw_1(X)),$$

  其中 $v_1(X) \neq 0$ 或 $w_1(x) \neq 0$. 记 $f_1 = v_1 + Yw_1$. 如果 $f_1(P) \neq 0$, 则 f_1 是单位且 $d = d_1$. 如果 $\overline{f_1}(P) \neq 0$, 则 $\overline{f_1}$ 是单位. 由于

$$f_1 = \mathrm{N}(f_1)\overline{f_1}^{-1} = (X - x)^{d_2} f_2 \overline{f_1}^{-1},$$

  其中 $f_2 \in K[X]$, $f_2(x) \neq 0$, 则 $f_2\overline{f_1}^{-1}$ 是单位且 $d = d_1 + d_2$. 当 $f_1(P) = \overline{f_1}(P) = 0$ 时, $(\alpha, \beta) = (v_1(x), w_1(x))$ 是齐次线性方程组

$$\begin{pmatrix} 1 & Y(P) \\ 1 & \overline{Y}(P) \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0$$

  的解. 由于 P 不是 2 阶点, 因此系数行列式 $(\overline{Y} - Y)(P) \neq 0$, 所以该方程组有唯一解 $\alpha = \beta = 0$, 从而与 $v_1(x), w_1(x)$ 不全为零矛盾.
- 如果 P 是一个 2 阶点且 $\operatorname{char} K \neq 2$, 则 $u = Y + \dfrac{1}{2}(a_1X + a_3) = \dfrac{1}{2}(Y - \overline{Y})$ 就是一个一致化参数.
  对通常的 Weierstrass 方程以及 u, P 应用容许的变量变换

$$(X, Y) \mapsto \left(X, Y - \frac{1}{2}(a_1X + a_3)\right)$$

可知，只需考虑

$$E: Y^2 = X^3 + a_2X^2 + a_4X + a_6, \quad u = Y, \quad P = (x_1, 0)$$

即可，其中 E 的右式有三个不同的零点 x_1, x_2, x_3. 由于

$$X - x_1 = \frac{(X-x_1)(X-x_2)(X-x_3)}{(X-x_2)(X-x_3)} = \frac{Y^2}{(X-x_2)(X-x_3)},$$

上式的分母在 P 点处不等于零. 记

$$f = (X-x_1)^{d_1} f_1 = \frac{Y^{2d_1}}{(X-x_2)^{d_1}(X-x_3)^{d_1}} f_1,$$

其中 $f_1 = v_1 + Yw_1$, $v_1, w_1 \in K[X]$ 且 $v_1(x_1), w_1(x_1)$ 不全为零. 如果 $f_1(P) \neq 0$, 则 $d = 2d_1$. 否则有 $v_1(x_1) = 0$, 因此 $v_1 = (X-x_1)v_2, v_2 \in K[X]$ 且 $w_1(x_1) \neq 0$, 从而有

$$f_1 = \frac{(X-x_1)(X-x_2)(X-x_3)v_2 + Yw_2}{(X-x_2)(X-x_3)} = Y\frac{v_2Y + w_2}{(X-x_2)(X-x_3)},$$

其中 $w_2 = w_1(X-x_2)(X-x_3)$ 且上式的第二个因子是单位，所以此时有 $d = 2d_1 + 1$.

- 如果 P 是一个 2 阶点且 $\operatorname{char} K = 2$, 则 $j \neq 0$. 此时一致化参数为 $Y + y$.
  对 E 作用变换

$$(X, Y) \mapsto \left(a_1^2X + \frac{a_3}{a_1}, a_1^3Y + t\right),$$

其中 $t = (a_1^2a_4 + a_3^2)/a_1^3$, 则可得曲线

$$E': Y^2 + XY = X^3 + a_2'X^2 + a_6',$$

并将点 P 作用为 (x', y'), 其中 $y' = a_1^{-3}(y+t)$ 而将 u 作用为 $a_1^3Y + t + y = a_1^3(Y + y')$. 由此可知只需对 E', $P = (0, y)$, $u = Y + y$ 进行证明即可，其中 $y^2 = a_6 \neq 0$. 与以上的证明类似的有

$$\begin{aligned} X &= (Y+y)^2\frac{X}{(Y+y)^2} = (Y+y)^2\frac{X}{Y^2+a_6} \\ &= (Y+y)^2\frac{X}{X^3+a_2X^2+XY} = \frac{(Y+y)^2}{X^2+a_2X+Y}, \end{aligned}$$

其中分母在 P 点处不等于零. 记

$$f = X^{d_1}f_1 = \frac{(Y+y)^{2d_1}}{(X^2+a_2X+Y)^{d_1}}f_1,$$

其中 $f_1=v_1+(Y+y)w_1$, $v_1,w_1\in K[X]$ 且 $v_1(0),w_1(0)$ 不全为零. 若 $f_1(P)\neq 0$, 则有 $d=2d_1$. 否则有 $v_1=Xv_2$, 其中 $v_2\in K[X]$ 且 $w_1(0)\neq 0$, 因此

$$f_1=(Y+y)\frac{(Y+y)v_2+w_1(X^2+a_2X+Y)}{X^2+a_2X+Y},$$

而上式的第二个因子就是单位, 所以此时有 $d=2d_1+1$. □

和通常情况一样, 一个离散赋值环在其分式域上定义了一个离散赋值 (或阶函数): 对于多项式 $f\neq 0$, 记 $\mathrm{ord}_P(f)$ 表示定理 2.11 中的整数 d. 为了方便, 约定 $\mathrm{ord}_P(0)=\infty$. ord_P 是 $K[E]$ 到 $\mathbb{Z}$ 上的可乘函数, 即 $\mathrm{ord}_P(fg)=\mathrm{ord}_P(f)+\mathrm{ord}_P(g)$, $f,g\in K[E]$. 同时可以通过令

$$\mathrm{ord}_P\left(\frac{f}{g}\right)=\mathrm{ord}_P(f)-\mathrm{ord}_P(g),$$

将其扩展定义到 $K(E)$ 上.

定义2.13　对于 $r\in K(E)$, $P\in E$, 称 $\mathrm{ord}_P(r)$ 为 r 在 P 点的阶. 如果 $\mathrm{ord}_P(r)>0$, 则称 P 是 r 的零点, 如果 $\mathrm{ord}_P(r)<0$, 则称 P 是 r 的极点. 零点和极点的重数为 $|\mathrm{ord}_P(r)|$.

要注意定理 2.11 的证明是构造性的, 由此可以确定有理函数在任意给定点处的阶.

例　设 $P=(x,y)\in E$. 下面确定 $X-x$ 所有的零点及其阶.

- 如果 P 不是 2 阶点, 则恰好有两个点的 X 坐标等于 x, 即 P, $\overline{P}$. 而 $X-x$ 是这两个点处局部环的一致化参数, 因此 $X-x$ 在 P, $\overline{P}$ 处有单零点, 而在 E 的其他点处的阶等于 0.
- 如果 $\mathrm{char}\,K\neq 2$, 而 P 是一个 2 阶点且 E 为标准形式, 则 $P=(x_1,0)$ 而

$$E: Y^2=(X-x_1)(X-x_2)(X-x_3),$$

其中 x_1,x_2,x_3 各不相同. 由于 Y 是一致化参数且 $(X-x_2)(X-x_3)$ 在 P 点处不等于零, 因此 $X-x_1$ 在 P 点处的阶等于 2. 在定理 2.11 中使用反向的变量变换容易看到: 当 E 不是标准形式时结论仍然成立, 即 $X-x$ 在 P 点处有 2 阶零点, 而在其他点处的阶等于零.

- 如果 $\mathrm{char}\,K=2$, P 是一个 2 阶点且 E 为标准形式 $Y^2+XY=X^3+a_2X^2+a_6$, 则有 $x=0$, $y^2=a_6\neq 0$. 这是唯一一个 X 坐标等于零的点, 其一致化参数是 $Y+y$. 正如在定理 2.11 的证明中所得到的, 有

$$X=(Y+y)^2\frac{1}{X^2+a_2X+Y},$$

而

$$\frac{1}{X^2+a_2X+Y}(P)=\frac{1}{y}$$

是有定义的且不等于零，所以 X 在 P 点处有 2 阶零点而在其他点处的阶等于零. 由于得到标准形式所采用的变量变换公式是具体的，因此该结论对一般形式的 E 仍然成立.

下面我们给出关于离散赋值的一个基本事实，其在后面的证明中是非常有用的.

命题2.14 设 ord 是域 L 上的离散赋值，则

$$\mathrm{ord}(f+g)\geqslant\min\{\mathrm{ord}f,\mathrm{ord}g\},\quad \forall f,g\in L$$

且当 $\mathrm{ord}f\neq\mathrm{ord}g$ 时等号成立. 更一般地有

$$\mathrm{ord}\left(\sum_{i=1}^{n}f_i\right)\geqslant\min\{\mathrm{ord}f_i:1\leqslant i\leqslant n\},\quad \forall n\in\mathbb{N},\quad f_1,\cdots,f_n\in L$$

且当最小值唯一时有等号成立.

证明 对于我们考虑的情况 (即椭圆曲线的情况)，该命题可由定理 2.11 直接得出. 对更一般的情况，要么如定理 2.11 那样首先定义离散赋值环，并类似地得到该命题；或者将该命题作为离散赋值定义的一部分，然后由此得到离散赋值环的概念. □

2.6 射影平面曲线

为得到椭圆曲线上的群运算规则，我们需要要求任意一条直线与曲线都有三个交点，因为两点之和与由这两点确定的直线与曲线的第三个交点有关. 更一般地说，我们要利用著名的 Bézout 定理 ([Bézout, 1779], p.32)：在考虑重数及其他适当①的情况下，次数分别为 m,n 的两条不同的曲线有 mn 个交点显然在仿射平面中这个定理并不成立：两条平行线甚至就没有交点. 为此我们需要引入某些点以使 Bézout 定理成立. 对每个平行直线类只需引入一个点即可，而得到的就是射影平面. 对于给定曲线，我们要详细说明引入的点，并由仿射曲线构造出对应的射影曲线.

① 首先是射影空间，其次是代数封闭域 —— 译者注.

定义2.15　集合 $K^3\backslash\{(0,0,0)\}$ 在等价关系

$$(x_1,y_1,z_1)\sim(x_2,y_2,z_2)\Longleftrightarrow\exists\lambda\in K^\times:(x_2,y_2,z_2)=\lambda(x_1,y_1,z_1)$$

下得到的等价类的全体被称为是 K 上的射影平面，记为 $P^2(K)$.

直观地说，射影平面中的“点”就是三维仿射空间中过原点的直线. 以下均用 (x,y,z) 表示整个等价类 $K^\times(x,y,z)$.

曲线现在就被定义为 $K[X,Y,Z]$ 中的多项式，但是我们必须确保：如果某个多项式在 (x,y,z) 处等于零，则其也必定在等价类 $K^\times(x,y,z)$ 中任意元素处等于零. 为此就要求该多项式是一个齐次多项式，即其每个单项式的次数是相同的. 记齐次多项式的全体为 $K[X,Y,Z]_{\text{hom}}$.

定义2.16　称射影平面中齐次不可约多项式 $C\in K[X,Y,Z]_{\text{hom}}$ 的全体零点构成的集合为一条射影平面曲线 . 如果对于曲线 C 上的点 P，有

$$\frac{\partial C}{\partial X}(P)=\frac{\partial C}{\partial Y}(P)=\frac{\partial C}{\partial Z}(P)=0,$$

则称 P 点是奇异的.

到目前为止，我们还并不清楚是否已经在仿射平面或仿射曲线上“添加上了适当的点”. 为此我们需要将 A^2 嵌入到 P^2 中，并定义多项式上相应的运算，使得“某个仿射点在仿射平面曲线上”当且仅当“其射影代表元在相应的射影平面曲线上”. 首先我们从点开始考虑. 设 U 表示 P^2 中所有 Z 坐标不为零的点所构成的集合，称 U 中的点为 P^2 的有限点. 由此可见通过除以 Z 坐标，U 中的点有唯一的 $(x,y,1)$ 形式的代表元，而把这样的点就看成是仿射点 (x,y).

定义2.17　分别称映射

$$A^2\to U,\quad (x,y)\mapsto(x,y)^*=(x,y,1)$$

及

$$U\to A^2,\quad (x,y,z)\mapsto(x,y,z)_*=\left(\frac{x}{z},\frac{y}{z},1\right)_*=\left(\frac{x}{z},\frac{y}{z}\right)$$

为点关于 Z 坐标的齐次化与非齐次化. 它们是 A^2 与 U 之间互逆的双射.

Z 坐标等于零的点被称为无穷远点，这是因为在上面定义中需要让分母趋于零. 它们就是射影平面中“新引入的点”. 现在我们要定义 $K[X,Y]$ 和 $K[X,Y,Z]_{\text{hom}}$ 之间的齐次和非齐次映射，使得“$P\in A^2(K)$ 是 $f\in K[X,Y]$ 的零点”的充要条件是

“P^* 是 f^* 的零点”. 同时 “$P \in U$ 是 $f \in K[X,Y,Z]_{\text{hom}}$ 的零点” 的充要条件是 “P_* 是 f_* 的零点”. 这里面第二个运算很容易定义：为保证$f(x,y,1)=0 \Longleftrightarrow f_*(x,y)=0$, 只需令 $f_* = f(X,Y,1)$ 即可. 另一方面，我们要求有 $f\left(\frac{x}{z},\frac{y}{z}\right)=0 \Longleftrightarrow f^*(x,y,z)=0$. 由于 $f^* = f\left(\frac{X}{Z},\frac{Y}{Z}\right)$ 并不是一个多项式，为此就必须乘以 Z 的某个幂次，即令 $f^* = Z^{\deg f} f\left(\frac{X}{Z},\frac{Y}{Z}\right)$.

定义2.18 分别称映射

$$K[X,Y] \to K[X,Y,Z]_{\text{hom}}, \quad f \mapsto f^* = Z^{\deg f} f\left(\frac{X}{Z},\frac{Y}{Z}\right)$$

及

$$K[X,Y,Z]_{\text{hom}} \to K[X,Y], \quad f \mapsto f_* = f(X,Y,1)$$

为多项式对 Z 坐标的齐次和非齐次化.

我们还要说明如果 C 是仿射曲线，则 C^* 是射影曲线，反之亦然. 换句话说要说明齐次与非齐次化是保持不可约性的. 实际上该结论是以下命题的推论. 由于该命题的证明比较简单，我们将其作为练习留给读者.

命题2.19 设 $f,g \in K[X,Y]$, $F,G \in K[X,Y,Z]_{\text{hom}}$，则

1. $(fg)^* = f^*g^*$
2. $(FG)_* = F_*G_*$
3. $(f^*)_* = f$
4. 如果 Z 不整除 F，则 $(F_*)^* = F$.

推论2.20 多项式 $C \in K[X,Y]$ 定义一条仿射曲线的充要条件是 C^* 也定义了一条射影曲线.

定义2.21 如果 C 是一条仿射曲线，则称 C^* 为 C 的射影闭包．C^* 由 C 上的点以及可能增加的某些无穷远点构成.

正如 2.1 节那样，我们要定义 C^* 上的有理函数. 为使定义合理，就必须要求这样的函数 r 必须是次数等于零的齐次函数：

$$r(\lambda P) = \lambda^0 r(P) = r(P), \quad \forall \lambda \in K^\times, \quad P \in C^*.$$

定义2.22　在 $K[C^*] := K[X,Y,Z]/(C^*)$ 的分式域中，由零函数和形如 $r = \dfrac{f}{g}$ 的函数构成的子域被称为是 C^* 上的有理函数域，记为 $K(C^*)$，其中 f,g 是次数相同的齐次多项式. 若有理函数 r 可表示为 $r = \dfrac{f}{g}$，其中 f,g 是次数相同的齐次多项式，且 $g(P) \neq 0$，　$P = (x,y,z) \in C^*$，则称 r 在 P 点处正则，或称 r 在 P 点处可定义. 所有在 P 点处正则的函数构成的环被称为是 C^* 在 P 点处的局部环，记为 $\mathcal{O}_P(C^*)$.

容易验证以上定义的集合的确分别是域和局部环. 下面通过扩展齐次和非齐次化映射将仿射曲线的有理函数域与其射影闭包的有理函数域相联系. 对于非齐次化映射而言，这是很简单的：如果

$$r = \frac{f}{g} \in K(C^*), \quad f,g \in K[C^*],$$

令

$$r_* = \frac{f_*}{g_*} = \frac{f(X,Y,1)}{g(X,Y,1)}.$$

对于 $r = \dfrac{f}{g} \in K(C)$，$f,g \in K[C]$，直接令 $r^* = \dfrac{f^*}{g^*}$ 是不行的. 这是由于 $f^* = Z^{\deg f} f\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)$ 的次数与 f 的次数是相同的，因此当 $\deg f \neq \deg g$ 时，f^*,g^* 是两个次数不同的齐次多项式，因此 $\dfrac{f^*}{g^*} \notin K(C^*)$. 为此同样我们需要乘以 Z 的某个幂次，即令

$$r^* = \frac{f(X/Z,Y/Z)}{g(X/Z,Y/Z)} = Z^{\deg g - \deg f}\frac{f^*}{g^*}.$$

上面的过程可能会引起歧义，这是因为当 $f \in K[C]$ 时，其有两种可能的齐次化形式：一方面 f 可以看成是一个多项式，因此 $f^* = Z^{\deg f} f\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)$ 就是其对应的齐次多项式. 另一方面，$f = \dfrac{f}{1}$ 是一个有理函数，$f^* = f\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)$就是对应的齐次有理函数. 由于当再次非齐次化时，$Z$ 的幂次并不会对 f 产生什么影响，所以我们可以根据需要任取其一.

命题2.23　由

$$K(C) \to K(C^*), \quad \frac{f}{g} \mapsto Z^{\deg g - \deg f}\frac{f^*}{g^*} = \frac{f\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)}{g\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)}$$

和

$$K(C^*) \to K(C), \quad \frac{f}{g} \mapsto \frac{f_*}{g_*} = \frac{f(X,Y,1)}{g(X,Y,1)}$$

定义的齐次和非齐次化映射是互逆的域同构. 如果 P 是 C 上的点, 则以上映射分别在 $\mathcal{O}_P(C)$, $\mathcal{O}_{P^*}(C^*)$ 上的限制是局部环之间两个互逆的环同构, 且对任意的 $r \in \mathcal{O}_P(C)$, 有 $r(P) = r^*(P^*)$.

证明 对第一个结论而言, 容易验证以上映射保持加法和乘法, 且它们是互逆的. 对第二个结论来说只要注意到 $f(X,Y) = f^*(X,Y,1)$ 即可. □

以上我们都是对 Z 坐标进行齐次和非齐次化. 当然该方法也可以同样地应用到 X,Y 坐标上. 这样就可以处理无穷远点. 由于任意一点的三个坐标中至少有一个不为零, 因此通过对这个不为零的坐标进行非齐次化, 该点就可以作为有限点来处理. 因此, 在需要的时候, 射影空间中的任何点都可以作为 "仿射点" 来处理. 在后面的几节中, 我们将特意地在仿射观点和射影观点之间转换.

2.7 射影椭圆曲线

利用前几节的知识, 射影椭圆曲线就可以被定义为仿射椭圆曲线的射影闭包. 这样前几节中得到的许多结论就可以推广到射影椭圆曲线上.

定义2.24 称形如

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

的方程为射影 Weierstrass 方程. 其判别式 Δ 以及 j 不变量的定义参见定义 2.7. 一个非奇异的射影 Weierstrass 方程就定义了一条射影椭圆曲线. 由

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$
$$E': Y^2Z + a_1'XYZ + a_3'YZ^2 = X^3 + a_2'X^2Z + a_4'XZ^2 + a_6'Z^3$$

定义的两条椭圆曲线同构是指: 通过以下的变量变换可以由 E 得到 E'

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} u^2X + rZ \\ u^3Y + u^2sX + tZ \\ Z \end{pmatrix},$$

其中 $u \in K^\times$, $r,s,t \in K$(并对最终得到的等式两边约去 u^6). 这样的变量变换被称为是容许的变量变换.

命题2.25　任何一个射影 Weierstrass 方程是不可约的. 其包含唯一的无穷远点 $\mathcal{O}=(0,1,0)$，且其奇异的充要条件是 $\Delta=0$.

证明　由 E_* 的不可约性及命题 2.19 直接可得 E 的不可约性. 设 $P=(x,y,z)\in E$ 是一个无穷远点，即 $z=0$，则有 $x^3=0$，因此 $P=\mathcal{O}$. 对于命题 2.25 的最后一个结论，由定理 2.10 知，只要证明 $\mathcal{O}$ 不可能是 Weierstrass 方程的奇异点即可. 事实上我们有

$$\frac{\partial E}{\partial Z}(0,1,0)=1\neq 0. \qquad \square$$

定理2.26　对于射影椭圆曲线 E 以及点 $P\in E$，环 $\mathcal{O}_P(E)$ 是一个离散赋值环.

证明　由定理 2.11 知该定理对有限点是成立的. 当 $P=\mathcal{O}$ 时，一致化参数可取为 $u=\dfrac{X}{Y}$. 现对 Y 坐标进行非齐次化：

$$E_*: Z+a_1XZ+a_3Z^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3.$$

由命题 2.23 可知只需证明 $u_*=X$ 是 $\mathcal{O}_{(0,0)}(E_*)$ 的一致化参数即可，其中 $(0,0)=\mathcal{O}_*$. 首先注意到在 $\mathcal{O}_{(0,0)}(E_*)$ 中有 X 整除 Z:

$$\begin{aligned}Z&=\frac{ZX^3}{X^3}\\&=\frac{ZX^3}{Z+a_1XZ+a_3Z^2-a_2X^2Z-a_4XZ^2-a_6Z^3}\\&=X^3\frac{1}{1+a_1X+a_3Z-a_2X^2-a_4XZ-a_6Z^2}\end{aligned}$$

其中分母在 $(0,0)$ 处并不等于零. 对于多项式 $f\in K[E_*]$，通过不断将 X^3 用 E_* 中相应的项代替，即可得 $f=r(Z)+s(Z)X+t(Z)X^2$，$r,s,t\in K[Z]$. 由此有

$$f=r_1(Z)Z^i+s_1(Z)Z^jX+t_1(Z)Z^kX^2,$$

其中 r_1,s_1,t_1 要么为零，要么不能被 Z 整除. 将 Z 用

$$\frac{X^3}{1+a_1X+a_3Z-a_2X^2-a_4XZ-a_6Z^2}$$

代替，则有

$$f=r_2(X,Z)X^{3i}+s_2(X,Z)X^{3j+1}+t_2(X,Z)X^{3k+2},$$

其中 r_2, s_2, t_2 为在 $(0,0)$ 处正则的有理函数，且它们要么是零函数，要么在 $(0,0)$ 处不等于零. 设 d 为 $3i$(若 $r_2 \neq 0$), $3j+1$(若 $s_2 \neq 0$) 和 $3k+2$(若 $t_2 \neq 0$) 中的最小值. 由于 d 恰好只是 $3i$, $3j+1$, $3k+2$ 中的某一个，则 $f = X^d f'$, 其中 f' 在 $(0,0)$ 处正则且不等于零. □

例　由上可知 $\frac{Z}{Y}$ 在 $\mathcal{O} \in E$ 处有 3 阶零点 (或者说当对 Y 进行非齐次化后，Z 在 $(0,0) \in E_*$ 处有 3 阶零点). 同样地，$\frac{Y}{Z}$ 或 $\frac{1}{Z}$ 在 $\mathcal{O}$ 处有 3 阶极点. 由于 $\mathrm{ord}_{\mathcal{O}}\left(\frac{X}{Y}\right) = 1, \mathrm{ord}_{\mathcal{O}}\left(\frac{Z}{Y}\right) = 3$, 因此 $\mathcal{O}$ 为有理函数 $\frac{X-xZ}{Y}$ 的单零点 (参见命题 2.14), 所以当 $x \in K$ 时，$\frac{X-xZ}{Z} = \frac{X-xZ}{Y}\frac{Y}{Z}$ 在 $\mathcal{O}$ 处有 2 阶极点. 该结论结合定义 2.13 后的例题，我们就得到了 $X-x$ 的所有零点.

2.8 除　子

为了更进一步地刻画有理函数的零点和极点，我们在由 E 上的点生成的自由交换群中，将该有理函数零点或极点的阶数作为该点处的系数，并对该自由交换群加以细致的研究.

定义2.27　E 的除子群是由 E 上的点所生成的自由交换群,

$$\mathrm{Div}(E) = \left\{ \sum_{P \in E} m_P \langle P \rangle : m_P \in \mathbb{Z}, \text{且除了有限个点} P \in E \text{外，有} m_P = 0 \right\}.$$

以上的求和应当看成是形式和，且要注意不要将其与 2.10 节定义的椭圆曲线上的加法相混淆. 若 $\Delta = \sum_{P \in E} m_P \langle P \rangle$ 是一个除子，则定义 $\deg \Delta = \sum_{P \in E} m_P$ 为其次数. 记 $\mathrm{Div}(E)$ 中由次数等于零的除子构成的子群为 $\mathrm{Div}^0(E)$. 对于有理函数 $r \neq 0$, 定义除子 $\mathrm{div}\, r = \sum_{P \in E} \mathrm{ord}_P(r) \langle P \rangle$, 而这样的除子被称为主除子.

在推论 2.30 中，我们将会证明有理函数只有有限多个零点和极点，因此 $\mathrm{div}\, r$ 的确是一个除子.

例　设 $P = (x, y, 1) \in E$, 由 2.5 和 2.7 节中的例子可知

$$\mathrm{div}\left(\frac{X-xZ}{Z}\right) = \langle P \rangle + \langle \overline{P} \rangle - 2\langle \mathcal{O} \rangle.$$

由于 $\mathrm{ord}_P(r_1 r_2) = \mathrm{ord}_P(r_1) + \mathrm{ord}_P(r_2)$, 则映射

$$\mathrm{div} : K(E)^\times \to \mathrm{Div}(E)$$

是一个交换群之间的同态, 因此由全体主除子组成的集合是除子群 $\mathrm{Div}(E)$ 的子群, 记为 $\mathrm{Prin}(E)$.

设 $\varphi: E \to E'$ 是椭圆曲线之间的同构, $\psi: K(E) \to K(E')$ 是相应的容许变量变换, 则由 φ 通过令 $\varphi(\langle P\rangle) = \langle\varphi(P)\rangle$ 可诱导出群同构: $\mathrm{Div}(E) \to \mathrm{Div}(E')$. 由 2.3 节知, 对于曲线 E 上的任意一点 P, ψ 构成 $\mathcal{O}_P(E)$ 和 $\mathcal{O}_{\varphi(P)}(E')$ 之间的同构, 因此有

$$\mathrm{div}(\psi(r)) = \varphi(\mathrm{div}(r)), \quad \forall r \in K(E)$$

且 φ 也是主除子群 $\mathrm{Prin}(E)$ 和 $\mathrm{Prin}(E')$ 之间的同构. 特别地有

$$\mathrm{div}(\overline{r}) = \overline{\mathrm{div}(r)},$$

所以 r 和 $\overline{r}$ 的零点和极点的重数是相同的 (要注意点可能是不同的).

下面我们计算有理函数的零点和极点, 其主要结论是:

定理2.28　*在计算重数的情况下, 有理函数的零点和极点个数相同, 即* $\mathrm{Prin}(E) \subseteq \mathrm{Div}^0(E)$.

首先由命题 2.23 知, 任何一个有理函数 r 都可以写成 $r = \dfrac{f\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right)}{g\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right)}$ 的形式, 其中 $f, g \in K[E_*]$, 因此只需对形如 $f^* = f\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right)$, $f \in K[E_*]$ 的有理函数完成定理的证明即可. 为此我们分别考虑 f^* 在有限点 (只能是零点) 和 $\mathcal{O}$(只能是极点) 处的阶.

引理2.29　*在计算重数的情况下,* $f \in K[E_*]$ *上有* $\deg(\mathrm{N}(f))$ *个零点, 其中* $\deg$ *表示* X *的次数.*

证明　记 $n = \deg(\mathrm{N}(f))$, $f\overline{f} = \mathrm{N}(f) = (X - x_1)\cdots(X - x_n)$. 由 2.5 节中的例子可知, $X - x_i$ 在 E_* 中有两个零点, 因此 $f\overline{f}$ 恰好有 $2n$ 个零点. 由于 f 和 $\overline{f}$ 的零点个数相同, 因此 f 的零点个数等于 n. □

由引理 2.29 显然可得以下结论:

推论2.30　*有理函数只有有限多个零点和极点.*

引理2.31　*如果* $f = v(X) + Yw(X) \in K[E_*]$, *则* f^* *在* $\mathcal{O}$ *处有一个* $\max\{2\deg v, 2\deg w + 3\}$ *阶极点.*

在文献 [Charlap and Robbins, 1988] 中，该结论被作为有理函数在 $\mathcal{O}$ 处阶的定义. 在这里我们从射影的观点给该定义更为确切的解释.

证明 首先考虑 $w=0$ 的情况. 记 $n=\deg v$，则

$$f^*=\sum_{i=0}^{n}a_i\frac{X^i}{Z^i},\quad a_n\neq 0.$$

我们要说明 $\mathrm{ord}_{\mathcal{O}}(f^*)=-2n$. 如果 $a_i\neq 0$，则由 2.7 节中的例题可知 $\mathrm{ord}_{\mathcal{O}}\left(a_i\frac{X^i}{Z^i}\right)=-2i$. 显然当 $i=n$ 时，$-2i$ 取到最小值 $-2n$，因此由命题 2.14 知 $\mathrm{ord}_{\mathcal{O}}(f^*)=-2n$.

当 $w\neq 0$ 时，有 $f^*=v\left(\frac{X}{Z}\right)+\frac{Y}{Z}w\left(\frac{X}{Z}\right)$，则当 $v\neq 0$ 时，由以上的证明可知

$$\mathrm{ord}_{\mathcal{O}}\left(v\left(\frac{X}{Z}\right)\right)=-2\deg v.$$

又由 2.7 节中的例题以及前面的证明可知

$$\mathrm{ord}_{\mathcal{O}}\left(\frac{Y}{Z}w\left(\frac{X}{Z}\right)\right)=\mathrm{ord}_{\mathcal{O}}\left(\frac{Y}{Z}\right)+\mathrm{ord}_{\mathcal{O}}\left(w\left(\frac{X}{Z}\right)\right)=-3-2\deg w.$$

如果 $v=0$，则证毕；否则由于 $-2\deg v$，$-3-2\deg w$ 不相等 (因为一个是偶数，一个是奇数)，因此由命题 2.14 知引理成立. □

利用下面的引理 2.32 就可以完成定理 2.28 的证明.

引理2.32 如果 $f=v(X)+Yw(X)\in K[E_*]$，则

$$\deg(\mathrm{N}(f))=\max\{2\deg v, 2\deg w+3\}.$$

证明 由定义 2.8 后的例题可知

$$\mathrm{N}(f)=v^2+\mathrm{Tr}(Y)wv+\mathrm{N}(Y)w^2.$$

由于

- $\deg(v^2)=2\deg v$ 是偶数.
- $\deg(\mathrm{N}(Y)w^2)=3+2\deg w$ 是奇数.
- 对于 $\deg(\mathrm{Tr}(Y)wv)\leqslant 1+\deg w+\deg v$ 有
  —— 当 $\deg w\geqslant\deg v$ 时，显然有 $1+\deg w+\deg v\leqslant\max\{2\deg v, 2\deg w+3\}$.
  —— 当 $\deg w<\deg v$，即 $\deg w+1\leqslant\deg v$ 时，也有 $1+\deg w+\deg v\leqslant\max\{2\deg v, 2\deg w+3\}$，

即 $\deg(\mathrm{Tr}(Y)wv) \leqslant 1 + \deg w + \deg v \leqslant \max\{2\deg v, 2\deg w + 3\}$.
由此可知 $\deg(\mathrm{N}(f)) = \max\{2\deg v, 3 + 2\deg w\}$. □

推论2.33　一个非常值的多项式至少有两个有限零点.

证明　由引理 2.29 和引理 2.32 显然可得. □

命题2.34　设 r 是一个有理函数且没有有限极点，则 r_* 一定为多项式.

证明　记 $r_* = v + wY, v, w \in K(X)$. 由命题 2.14 知，存在着以下两种可能的情况：v, w 都没有极点 (在证明过程中，"极点" 就是指 "有限极点")，则此时 v, w 必定均为多项式，证毕；或者 v, w 有相同的极点. 下面说明第二种情况是不可能出现的. 由于容许的变量变换保持多项式以及极点的存在性，因此为简化证明过程，不妨设 E 是标准形式. 由于 r_* 没有极点，因此 $\overline{r}_*$ 也没有极点，且

$$r_* - \overline{r}_* = (2Y + a_1X + a_3)w.$$

由此可知如果 $P = (x, y)$ 为 w 的极点，则 P 必定是 $2Y + a_1X + a_3$ 的零点，即 P 是一个 2 阶点.

1. 当 $\mathrm{char}\, K \neq 2$ 时，存在着 3 个 2 阶点. 由引理 2.29 以及引理 2.32 知，每个 2 阶点均为 $2Y + a_1X + a_3$ 的单零点，因此 P 为 w 的单极点. 另一方面，记 $w = \dfrac{f}{g}$，其中 f, g 为 $K[X]$ 中互质的多项式. 由于 P 为 w 的单极点，因此 $X - x \mid g$，$X - x \nmid f$. 由 2.5 节的例子知，$X - x$ 在 P 点处有 2 阶零点，因此 w 在 P 点处至少有 2 阶极点，矛盾.
2. 当 $\mathrm{char}\, K = 2$ 时，必定有 $j \neq 0$ 且 P 为唯一的 2 阶点. 设 E_* 为标准形式

$$Y^2 + XY = X^3 + a_2X^2 + a_6,\ a_6 \neq 0,$$

则 $P = (0, \sqrt{a_6})$. 由于 $r_* - \overline{r}_* = Xw \in K(X)$ 没有极点，因此 $r_* - \overline{r}_*$ 是一个多项式 $w_1X + w_0$，其中 $w_1 \in K[X], w_0 \in K$. 更进一步地有 $w_0 \neq 0$(否则 w 在 P 点处就没有极点). 由此可知 w 在 P 点处有一个 2 阶极点. 由命题 2.14 知 v 在 P 点处也有 2 阶极点，且同样地可以得出 Xv 是一个多项式 $v_1X + v_0$，其中 $v_1 \in K[X]$，$v_0 \in K^\times$. 因此

$$\begin{aligned} r_* &= \frac{v_1X + v_0}{X} + \frac{w_1X + w_0}{X}Y \\ &= (v_1 + w_1Y) + w_0\frac{Y + \frac{v_0}{w_0}}{X}. \end{aligned}$$

由于 X 在 P 点处有 2 阶零点而 r_* 没有极点，因此 $Y+\frac{v_0}{w_0}$ 在 P 点处至少有一个 2 阶零点，即 $\frac{v_0}{w_0}=\sqrt{a_6}$. 但由定理 2.11 的证明过程可知 $Y+\sqrt{a_6}$ 是 $\mathcal{O}_P(E_*)$ 的一致化参数，因此 $Y+\sqrt{a_6}$ 在 P 点处只有一个单零点，矛盾. □

推论2.35 设 Δ 是一个主除子，则以 Δ 为除子的有理函数至多只相差 K 中一个非零常数因子.

证明 设 $g, \tilde{g}$ 都是以 Δ 为除子的有理函数，则 $r=g/\tilde{g}$ 的除子等于零. 由命题 2.34 知，r_* 是一个多项式，同时又由推论 2.33 知其必为一个常数. □

下面我们将要讨论有理函数会有什么样的零点和极点，也就是什么样的除子是主除子. 更一般地，我们考虑 $\mathrm{Div}(E)$ 模主除子群所得的商群. 由定理 2.28 知只需考虑次数为零的除子即可. 由此得到以下的定义.

定义2.36 如果两个除子 Δ_1, Δ_2 满足

$$\Delta_1-\Delta_2 \in \mathrm{Prin}(E),$$

则称它们是线性等价的，记为 $\Delta_1 \sim \Delta_2$. 称 $\mathrm{Pic}(E) := \mathrm{Div}(E)/\mathrm{Prin}(E)$ 为 E 的 Picard 群或除子类群，而称 $\mathrm{Pic}^0(E) := \mathrm{Div}^0(E)/\mathrm{Prin}(E)$ 为除子类群的零次部分.

术语 "线性等价" 看上去似乎让人感到困惑，因为主除子是来源于有理函数，那么此时称其为 "有理等价" 好像更为合理. 事实上，椭圆曲线上的所有有理函数的除子都可由最简单的线性函数的除子来构造. 在 2.10 节研究除子的一般理论之前，我们将对直线的除子加以细致的研究. 而由于直线的零点和极点是很容易计算得到的，由此就可以来处理 $\mathrm{Pic}^0(E)$ 中的除子.

2.9 直　线

定义2.37 一条(仿射)直线 l 是指一个一次多项式，即 $l=\alpha X+\beta Y+\gamma$，其中 α, β 不全为零. 通过乘以 $K^\times$ 中的某个恰当的因子，可不妨设 α 或 β 等于 1.

把直线看成是有理函数，有两个问题需要考虑：1. 给定一条直线，能否有效计算其除子？2. 给定一个除子或除子中的某些项，是否存在以其为除子的直线？

对于第一个问题，前面一节中的例题给出了部分回答：如果 $l=X-x$，则

$$\mathrm{div}(l^*)=\langle P\rangle+\langle \overline{P}\rangle-2\langle \mathcal{O}\rangle,$$

其中 P_* 是 E_* 上某个以 x 为 X 坐标的点. 这些点可以通过把 x 代入仿射 Weierstrass 方程，求出对应的 $Y(P_*)$ 和 $Y(\overline{P_*})$ 来得到.

当 $\beta \neq 0$ 时 (此时可设 $\beta = 1$)，也有类似结论.

引理2.38 设 $l = Y - (mX + b)$, $P = (x, y, 1)$ 是 $l^* \cap E$ 中的点，则 $\mathrm{ord}_P(l^*)$ 等于 x 作为单变量多项式 $E_*(X, mX + b)$ 零点的重数.

证明 一方面，由于

$$E_*(X,T) = T^2 - \mathrm{Tr}(Y)T + \mathrm{N}(Y) = (Y - T)(\overline{Y} - T),$$

因此

$$E_*(X, mX + b) = (Y - (mX + b))(\overline{Y} - (mX + b)) = l\bar{l};$$

另一方面，由于 $E_*(X, mX + b)$ 是三次多项式，因此可以分解为三个线性因子的乘积：

$$E_*(X, mX + b) = -(X - x_1)(X - x_2)(X - x_3),$$

其中 x_1, x_2, x_3 可能相同. 由此可知

$$\begin{aligned}\mathrm{div}(l^*\bar{l}^*) &= \mathrm{div}(l^*) + \mathrm{div}(\bar{l}^*)\\ &= \mathrm{div}((Y - (mX + b))^*) + \mathrm{div}((\overline{Y} - (mX + b))^*)\\ &= \langle P_1\rangle + \langle \overline{P_1}\rangle + \langle P_2\rangle + \langle \overline{P_2}\rangle + \langle P_3\rangle + \langle \overline{P_3}\rangle - 6\langle \mathcal{O}\rangle,\end{aligned}$$

其中 P_i 是 $(X - x_i)^*$ 在 E 上的零点.

记 d 表示 x 作为 $E_*(X, mX + b)$ 零点的重数，则 x 在 x_1, x_2, x_3 中出现 d 次. 同时由 P_i 的定义知，$x = x_i$ 的充要条件是 $P \in \{P_i, \overline{P_i}\}$. 下面我们分两种情况加以讨论：

1. 当 $P = \overline{P}$ 时，$x = x_i$ 就意味着 $P = P_i = \overline{P_i}$，则 P 在除子中出现 $2d$ 次，因此

$$2d = \mathrm{ord}_P(l^*) + \mathrm{ord}_P(\bar{l}^*) = \mathrm{ord}_P(l^*) + \mathrm{ord}_{\overline{P}}(l^*) = 2\mathrm{ord}_P(l^*).$$

2. 当 $P \neq \overline{P}$ 时，$x = x_i$ 意味着 P 只是 $P_i, \overline{P_i}$ 中的某一个，因此

$$d = \mathrm{ord}_P(l^*) + \mathrm{ord}_P(\bar{l}^*) = \mathrm{ord}_P(l^*) + \mathrm{ord}_{\overline{P}}(l^*).$$

而且过 $P_*, \overline{P_*}$ 的直线只有一条，即 $X - x$. 由于 P 在直线 l^* 上，而即使在相差一个常数因子的情况下，l 与 $(X - x)^*$ 仍然是不同的，因此 $\overline{P} \notin l^*$，所以有 $\mathrm{ord}_{\overline{P}}(l^*) = 0$. □

利用以上的引理就可以得到计算 $l = Y - (mX + b)$ 除子的方法：首先计算 $E_*(X, mX + b)$ 的根 x_1, x_2, x_3，然后令 $P_i = (x_i, mx_i + b, 1)$，则 $\text{div}(l^*) = \langle P_1\rangle + \langle P_2\rangle + \langle P_3\rangle - 3\langle\mathcal{O}\rangle$.

推论2.39 设 l 是一条直线，则存在可以有效计算的有限点 P, Q 和 R，满足

$$\text{div}(l^*) = \begin{cases} \langle P\rangle + \langle \overline{P}\rangle - 2\langle\mathcal{O}\rangle, & l = X - x, \\ \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle, & l = Y - (mX + b). \end{cases}$$

可以看出 "$-3\langle\mathcal{O}\rangle$" 来自于对 Z 的齐次化过程，因此该推论就是关于椭圆曲线和直线交点的 Bézout 定理：次数分别为 1 和 3 的两条曲线必有三个交点. 在第一种情况中就是 $P, \overline{P}, \mathcal{O}$，在第二种情况下就是 P, Q 和 R.

下一个问题是如何寻找在给定点处有指定阶的直线. 这样就可以通过加上直线的除子来得到同一除子类中除子的适当表示. 由于两个不同的点就可以确定一条直线，因此为确定该直线，很自然地就可以首先确定两个点. 也就是说问题可归结为：对于给定的两点 P, Q(可能相同)，是否存在直线 l 以及点 R，使得 $\text{div}(l^*) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle$？如果这样的直线是存在的，那又如何确定呢？

定理2.40 设 P, Q 是椭圆曲线 E 上不全为无穷远点 $\mathcal{O}$ 的两点，则存在可以有效计算的唯一的一条直线 l 以及唯一的点 R，满足

$$\text{div}(l^*) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle.$$

证明 若 $P = (x, y, 1)$, $Q = \mathcal{O}$(反之亦然)，则由推论 2.39 知 $l = X - x$, $R = \overline{P}$.

若 $P = (x_1, y_1, 1)$, $Q = (x_2, y_2, 1)$ 是两个不同的点，则过 P, Q 存在唯一的直线 l. 如果 $P = \overline{Q}$，即 $x_1 = x_2$，则 $l = X - x_1$, $R = \mathcal{O}$. 否则 $l = Y - (\lambda X + \mu)$，其中

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = y_1 - \lambda x_1,$$

而 R 可以通过前面提及的方法求出. □

当 $P = Q$ 时的证明比较困难. 什么样的直线在给定点处有一个多重零点？实际上这样的直线必定就是切线，但证明这一结论需要一些预备知识.

定义2.41 设 $P = (x, y)$ 是仿射曲线 C 上的一个非奇异点，则定义 C 在 P 点处的切线为

$$\frac{\partial C}{\partial X}(P)(X - x) + \frac{\partial C}{\partial Y}(P)(Y - y).$$

注意由非奇异点的定义知至少有一个偏导数不等于零，因此以上关于切线的定义是合理的.

例 设 E 是一条仿射椭圆曲线，$P=(x,y)$，则 E 在 P 点处的切线为

$$(a_1y-(3x^2+2a_2x+a_4))(X-x)+(2y+a_1x+a_3)(Y-y).$$

以下的引理把 P 点处的切线与 P 点的阶相联系. 其结论对任意曲线都是成立的，但这里我们只对椭圆曲线的情况加以证明.

引理2.42 设 P 是椭圆曲线上的有限点，l 为一条直线，则 l 是 P 点处的切线的充要条件是 $\mathrm{ord}_P(l^*)\geqslant 2$.

证明 显然点 P 不在直线 l^* 上的充要条件是 $\mathrm{ord}_P(l^*)=0$. 不妨设 $P=(x,y,1)\in l^*$，且 l 的形式是 $\alpha(X-x)+\beta(Y-y)$，其中 α,β 中有一个等于 1. 下面我们分两种情况讨论：

1. 当 $P=\overline{P}$ 时，有 $2y+a_1x+a_3=0$. 此时切线为 $t=X-x$ 且 $\mathrm{ord}_P(t^*)=2$. 反之设 $\mathrm{ord}_P(l^*)\geqslant 2$ 且由于容许的变量变换是仿射变换且保持直线和相切性不变，因此不妨设 E 为表 2.2 所示的某一标准形式. 由 2.5 节知 $Y-y$ 就是一致化参数，因此 $\mathrm{ord}_P((Y-y)^*)=1$. 而已知 $\mathrm{ord}_P((X-x)^*)=2$，因此由命题 2.14 知只有当 $\beta=0$ 时才可能有 $\mathrm{ord}_P(l^*)\geqslant 2$，因此 $l=t$.
2. 当 $P\neq\overline{P}$ 时，若 $\beta=0$，则 l 不是切线且由推论 2.39 知 $\mathrm{ord}_P(l^*)=1$. 因此可设 $\beta=1$，则直线 l 为切线的充要条件是

$$\alpha=\frac{\dfrac{\partial E_*}{\partial X}(P_*)}{\dfrac{\partial E_*}{\partial Y}(P_*)}.$$

又由引理 2.38 知 $\mathrm{ord}_P(l^*)\geqslant 2$ 的充要条件是 $E_*(X,-\alpha(X-x)+y)$ 在 x 处有多重零点，即

$$\frac{\partial E_*(X,-\alpha(X-x)+y)}{\partial X}(x)=\frac{\partial E_*}{\partial X}(x,y)-\alpha\frac{\partial E_*}{\partial Y}(x,y)=0,$$

即 $\alpha=\dfrac{\dfrac{\partial E_*}{\partial X}(P_*)}{\dfrac{\partial E_*}{\partial Y}(P_*)}$. □

利用以上的预备知识就可以完成定理 2.40 的证明：对于给定的点 P，存在唯一的在 P 点处阶大于等于 2 的直线，即在 P 点处的切线. □

2.10 Picard 群

本节的目的是对 $\mathrm{Pic}(E)$ 中的每一个元素找到一个 "简单" 的代表元. 同时我们证明 $\mathrm{Pic}^0(E)$ 与椭圆曲线 E 上的点之间存在一个双射, 因此我们可以通过 $\mathrm{Pic}^0(E)$ 中的群运算来定义 E 上的运算.

定理2.43 *设 $\Delta \in \mathrm{Div}(E)$, 则存在唯一的点 $P \in E$ 满足*

$$\Delta \sim \langle P\rangle + (\deg\Delta - 1)\langle \mathcal{O}\rangle.$$

证明 设除子 $\Delta = \sum_{P\in E} m_P\langle P\rangle$, 称 $|\Delta| = \sum_{P\in E\setminus\{\mathcal{O}\}} |m_P|$ 为 Δ 的范数. 首先是通过对除子的范数进行归纳来证明命题: 如果 $|\Delta| > 1$, 则通过添加某条适当直线的除子, 就可以在 Δ 所在的除子类中, 找到另一个具有更小范数的除子. 由于该除子与 Δ 在同一个除子类中, 因此该除子与 Δ 线性等价. 其具体过程如下:

- 如果存在两个点 P, Q, 满足 m_P, $m_Q > 0$. 设 l 是过 P, Q 的直线, 则通过在 Δ 中减去 l 的除子, 就可使得 $|m_P|$, $|m_Q|$ 减少 1. 若 $\mathrm{div}(l^*) = \langle P\rangle + \langle Q\rangle - 2\langle \mathcal{O}\rangle$ 时, 则范数 $|\Delta|$ 减少 2. 否则 $\mathrm{div}(l^*) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle \mathcal{O}\rangle$ 而 $|m_R|$ 至多增加 1. 无论是哪种情况, $|\Delta|$ 都至少减少 1.
- 如果存在两个点 P, Q 满足 m_P, $m_Q < 0$, 则通过加上过 P, Q 直线的除子, 类似于上面的讨论也有 $|\Delta|$ 至少减少 1.

以下只要考虑 Δ 的形式为 $m\langle P\rangle - n\langle Q\rangle + o\langle \mathcal{O}\rangle$ 时的情况, 其中 m, $n \geqslant 0$.

- 如果 $m \geqslant 2$, 则在 Δ 中减去 P 点处切线的除子: $2\langle P\rangle + \langle R\rangle - 3\langle \mathcal{O}\rangle$. 如果 $n \geqslant 2$, 则加上 Q 点处切线的除子. 不管是哪种情况, $|\Delta|$ 都至少减少 1.
- 如果 $\Delta = \langle P\rangle - \langle Q\rangle + o\langle \mathcal{O}\rangle$, 则加上过点 $Q, \overline{Q}$ 直线的除子 $\langle Q\rangle + \langle \overline{Q}\rangle - 2\langle \mathcal{O}\rangle$, 得到的除子 $\langle P\rangle + \langle \overline{Q}\rangle + (o-2)\langle \mathcal{O}\rangle$ 与 Δ 有相同的范数. 而由于此时 $m_P = m_{\overline{Q}} = 1 > 0$, 因此该除子属于已经讨论的情况, 因此其范数可以进一步降低.
- 如果 m, n 中有一个等于零, 则已经证毕.

通过以上的过程得到的除子 $\Delta' \sim \Delta$ 且范数至多为 1. 如果 $|\Delta'| = 0$, 则 $\Delta' = \langle \mathcal{O}\rangle + (\deg\Delta - 1)\langle \mathcal{O}\rangle$ 就是所需的形式. 如果 $\Delta' = -\langle P\rangle + (\deg\Delta + 1)\langle \mathcal{O}\rangle$, 则通过加上过 $P, \overline{P}$ 直线的除子 $\langle P\rangle + \langle \overline{P}\rangle - 2\langle \mathcal{O}\rangle$ 可得除子 $\langle \overline{P}\rangle + (\deg\Delta - 1)\langle \mathcal{O}\rangle$. 这样就完成了存在性的证明.

为证明唯一性, 我们假设 $\Delta \sim \langle P\rangle - o\langle \mathcal{O}\rangle \sim \langle Q\rangle - o\langle \mathcal{O}\rangle$, 则 $\langle P\rangle - \langle Q\rangle$ 就是一个主除子. 与证明存在性类似地, 减去过 $P, \overline{P}$ 直线的除子 $\langle P\rangle + \langle \overline{P}\rangle - 2\langle \mathcal{O}\rangle$, 可得

$$\langle P\rangle - \langle Q\rangle - (\langle P\rangle + \langle \overline{P}\rangle - 2\langle \mathcal{O}\rangle) = -\langle Q\rangle - \langle \overline{P}\rangle + 2\langle \mathcal{O}\rangle.$$

再加上过 $\overline{P},Q$ 直线的除子 $\langle\overline{P}\rangle+\langle Q\rangle+\langle R\rangle-3\langle\mathcal{O}\rangle$，可得主除子

$$-\langle Q\rangle-\langle\overline{P}\rangle+2\langle\mathcal{O}\rangle+(\langle\overline{P}\rangle+\langle Q\rangle+\langle R\rangle-3\langle\mathcal{O}\rangle)=\langle R\rangle-\langle\mathcal{O}\rangle.$$

如果 $P\neq Q$, 则 $\overline{P}$ 与 Q 不共轭且由推论 2.39 知 R 是有限点. 由于 $\langle R\rangle-\langle\mathcal{O}\rangle$ 是主除子，设 r 为 $\langle R\rangle-\langle\mathcal{O}\rangle$ 对应的有理函数. 由于 r 没有有限极点，因此由命题 2.34 知其是一个多项式. 但是 r 只有一个有限零点，因此与推论 2.33 矛盾，所以 $P=Q$. 证毕. □

推论2.44　*对于 $\Delta\in\mathrm{Pic}^0(E)$, 存在唯一的 $P\in E$ 满足 $\Delta\sim\langle P\rangle-\langle\mathcal{O}\rangle$. 映射*

$$\sigma:\mathrm{Pic}^0(E)\to E,\quad \Delta\mapsto P$$

及

$$\kappa:E\to\mathrm{Pic}^0(E),\quad P\mapsto\Delta$$

是互逆的双射.

2.11　群　法　则

现在我们可以定义椭圆曲线上的群运算规则. 首先我们从几何的观点加以考察 (参见图 2.2), 并粗略地给出算法的思想：为定义两个点 P, Q 的和，我们过这两点作一条线 (如果 $P=Q$, 则就是 P 点处的切线), 确定其与椭圆曲线的第三个交点 R, 则令 $P+Q=\overline{R}$. $\overline{R}$ 的几何解释就是，过点 R 作一条垂线，则其与曲线的另一个交点就是点 $\overline{R}$ (第三个交点就是 $\mathcal{O}$).

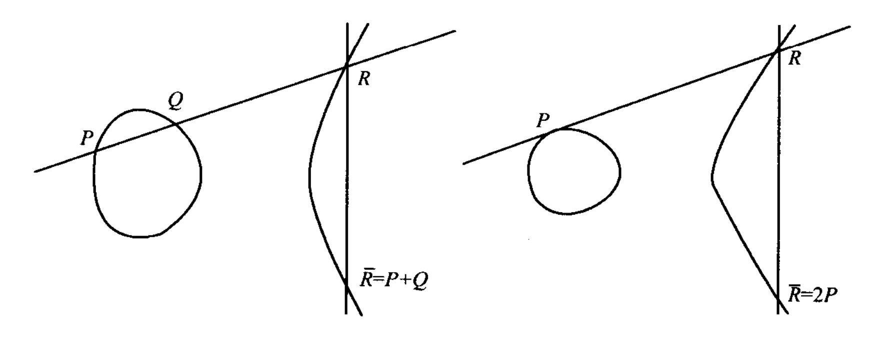


图 2.2　椭圆曲线上点加与倍点的计算

本节要完成两个任务：①验证 E 在这样定义的运算下构成群；②给出两个点相加的计算公式. 为此我们首先给出以上运算的正式定义.

定义2.45 在椭圆曲线上定义运算 "+" 如下:

- $\mathcal{O}+\mathcal{O}=\mathcal{O}$.
- 对不全为无穷远点的两个点 P, Q, 由定理 2.40 知存在唯一直线 l 以及唯一的点 R, 满足

  $$\operatorname{div} l^* = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle,$$

  令 $P+Q:=\overline{R}$.

定理2.46 $(E,+)$ 是一个交换群.

证明 群定义中的大多数要求可以通过直接验证得以证明:

- $+$ 是交换的.
- $\mathcal{O}$ 是单位元. 如果 P 是无穷远点, 则由定义知 $P+\mathcal{O}=\mathcal{O}=P$; 否则 $P=(x,y,1)$ 而过点 P, $\mathcal{O}$ 的直线为 $l=X-x$, 其除子为 $\operatorname{div} l^*=\langle P\rangle+\langle\mathcal{O}\rangle+\langle\overline{P}\rangle-3\langle\mathcal{O}\rangle$, 因此 $P+\mathcal{O}=\overline{\overline{P}}=P$.
- $-P=\overline{P}$ 是 P 的逆元. 如果 P 是无穷远点, 则这是显然的. 如果 $P=(x,y,1)$, 则由 $\operatorname{div}((X-x)^*)=\langle P\rangle+\langle\overline{P}\rangle+\langle\mathcal{O}\rangle-3\langle\mathcal{O}\rangle$ 知 $P+\overline{P}=\overline{\mathcal{O}}=\mathcal{O}$.

唯一比较困难的是结合律的证明. 这点可以通过代数曲线理论 (参见 [Fulton, 1969], p.125) 得以证明. 在此我们并不采用这样的方法, 而是通过证明 $(E,+)$ 与 $\operatorname{Pic}^0(E)$ 同构来完成. 由 2.10 节知

$$\kappa: E\to \operatorname{Pic}^0(E),\quad P\mapsto\langle P\rangle-\langle\mathcal{O}\rangle$$

是一个双射, 因此只需证明 κ 与 E 上的运算是相容的即可, 即要证明

$$\kappa(P+Q)=\kappa(P)+\kappa(Q),\quad \forall P,\ Q\in E.$$

当 $P=Q=\mathcal{O}$ 时, 这是显然的. 因此不妨设 P, Q 中至少有一个是有限点. 设 l 是除子为

$$\operatorname{div} l^* = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle$$

的直线, 则 $P+Q=\overline{R}$. 下面需要证明

$$\langle\overline{R}\rangle-\langle\mathcal{O}\rangle\sim\langle P\rangle+\langle Q\rangle-2\langle\mathcal{O}\rangle,$$

也就是要证明 $\langle P\rangle+\langle Q\rangle-\langle\overline{R}\rangle-\langle\mathcal{O}\rangle$ 是一个主除子. 若 l' 是以 $\langle R\rangle+\langle\overline{R}\rangle-2\langle\mathcal{O}\rangle$ 为除子的直线, 则

$$\operatorname{div}\frac{l^*}{l'^*}=\langle P\rangle+\langle Q\rangle-\langle\overline{R}\rangle-\langle\mathcal{O}\rangle$$

就是一个主除子. □

推论2.47

1. $(E,+)$ 与 $\mathrm{Pic}^0(E)$ 同构.
2. 如果 E, E' 同构, 则 $(E,+), (E',+)$ 也同构.

证明　第一个就是前面证明的结论. 同时由 2.8 节中的讨论可知椭圆曲线之间的同构与其除子理论是相容的, 因此第二个结论也成立. □

为实现椭圆曲线上的群运算, 需要得到 $P+Q$ 坐标与 P, Q 坐标之间的关系. 如果 P, Q 中存在无穷远点, 则 $P+Q$ 的计算是显然的. 现设 $P=(x_1,y_1,1)$, $Q=(x_2,y_2,1)$. 如果 $Q=\overline{P}$, 即 $x_1=x_2$, $y_2=-y_1-a_1x-a_3$, 则 $P+Q=\mathcal{O}$. 否则过 P,Q 点的直线为

$$l=Y-(\lambda X+\mu),$$

其中

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & P\neq Q,\\[2mm] \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & P=Q(\text{参见定义 2.41 后的例题}),\end{cases}$$

$$\mu=y_1-\lambda x_1.$$

l 与 E 的第三个交点 $R=(x_3,y_3,1)$ 可以通过引理 2.38 中证明的式子

$$-(X-x_1)(X-x_2)(X-x_3)=E_*(X,\lambda X+\mu)$$

计算得出: 在上式两边 X^2 的系数分别为 $x_1+x_2+x_3$ 和 $\lambda^2+a_1\lambda-a_2$, 因此

$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2,\quad y_3=\lambda x_3+\mu,$$

从而有

$$P+Q=\overline{R}=(x_3,-y_3-a_1x_3-a_3)=(x_3,-(\lambda+a_1)x_3-a_3-\mu).$$

对于 $P=(x_1,y_1)=(x,y), Q=(x_2,y_2)$ 且 $P\neq -Q$, 表 2.3 至表 2.5 总结了一般情况以及特征等于 2 时标准形式椭圆曲线上的点加公式. 其中唯一需要解释的是表 2.4 中计算倍点 X 坐标的公式. 由表 2.3 中的计算公式可知

$$\begin{aligned}x_3&=\left(\frac{x^2+y}{x}\right)^2+\frac{x^2+y}{x}+a_2\\&=\frac{x^4+y^2+x^3+xy+a_2x^2}{x^2}\\&=\frac{x^4+a_6}{x^2}.\end{aligned}$$

表 2.3 椭圆曲线 $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ 的点加公式

$$x_3 = \begin{cases} \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\dfrac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2, & P \neq Q \\ \left(\dfrac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\right)^2 + a_1\left(\dfrac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\right) - a_2 - 2x, & P = Q \end{cases}$$

$$y_3 = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 - (a_1x_3 + a_3), & P \neq Q \\ \dfrac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}(x - x_3) - y - (a_1x_3 + a_3), & P = Q \end{cases}$$

表 2.4 char $K = 2, j \neq 0$ 时，椭圆曲线 $Y^2 + XY = X^3 + a_2X^2 + a_6$ 的点加公式

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right) + a_2 + x_1 + x_2, & P \neq Q \\ x^2 + \dfrac{a_6}{x^2}, & P = Q \end{cases}$$

$$y_3 = \begin{cases} \dfrac{y_1 + y_2}{x_1 + x_2}(x_1 + x_3) + y_1 + x_3, & P \neq Q \\ \dfrac{x^2 + y}{x}x_3 + x^2 + x_3, & P = Q \end{cases}$$

表 2.5 char $K = 2, j = 0$ 时，椭圆曲线 $Y^2 + a_3Y = X^3 + a_4X + a_6$ 的点加公式

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2, & P \neq Q \\ \left(\dfrac{x^2 + a_4}{a_3}\right)^2, & P = Q \end{cases}$$

$$y_3 = \begin{cases} \dfrac{y_1 + y_2}{x_1 + x_2}(x_1 + x_3) + y_1 + a_3, & P \neq Q \\ \dfrac{x^2 + a_4}{a_3}(x + x_3) + y + a_3, & P = Q \end{cases}$$

其中最后一个等式成立的原因是：由于 (x, y) 为 E 上的点，因此有 $y^2 + xy + x^3 + a_2x^2 = a_6$.

到目前为止，我们一直都在讨论代数闭域上的椭圆曲线. 但是我们更感兴趣的

域 (在其中能够有效地进行计算，从而适用于密码学领域) 是有限域. 由 $P+Q$ 和 $-P$ 坐标的计算公式表明如果我们对坐标在某个子域 $k \subseteq K$ 中的点进行加法和求逆运算，则所得点的坐标依然在 k 中. 由此得到以下一般域上的第一个结果.

推论2.48 设 K 是一个域 (未必是代数闭域)，E 是定义在 K 上的椭圆曲线，则 $(E,+)$ 是一个群，其中加法运算是由以上公式定义的.

例 取四元域 $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$，其中 α 是 $\mathbb{F}_4$ 乘法群的生成元，则

$$\alpha^2=\alpha^{-1}=\alpha+1,(\alpha+1)^2=\alpha^4=\alpha,\alpha(\alpha+1)=\alpha^3=1.$$

取 $\mathbb{F}_4$ 上的椭圆曲线 $E:Y^2+Y=X^3+X+1$.

由于 $j=0$，因此由 2.5 节知其不存在 2 阶点. 下面考虑 E 上的有限点 $P=(x,y)$. 若 $x=0$ 或 $x=1$，则 $y^2+y=1$，因此 $y=\alpha$ 或 $y=\alpha+1$. 若 $x=\alpha$ 或 $x=\alpha+1$，则 $y^2+y=x$，但该方程无解.

由以上计算可知 E 上的点为：$P_1=(0,\alpha)$，$P_2=(0,\alpha+1)$，$P_3=(1,\alpha)$，$P_4=(1,\alpha+1)$ 以及 $\mathcal{O}$，因此该群必定是 5 阶循环群且任意 P_i 均为生成元. 下面我们再通过计算 P_1 的倍点来加以验证. 由表 2.5 中的公式可知当 $P=(x_1,y_1)$，$Q=(x_2,y_2)\neq\overline{P}$ 时，$R=P+Q=(x_3,y_3)$，其中

$$\overline{P}=(x_1,y_1+1),$$
$$x_3=\begin{cases}\left(\dfrac{y_1+y_2}{x_1+x_2}\right)^2+x_1+x_2, & P\neq Q,\\ x_1^4+1=x_1+1, & P=Q,\end{cases}$$
$$y_3=\begin{cases}\left(\dfrac{y_1+y_2}{x_1+x_2}\right)^3+\left(\dfrac{y_1+y_2}{x_1+x_2}\right)x_2+y_1+1, & P\neq Q,\\ x_1^2+y_1, & P=Q,\end{cases}$$

因此

$$\begin{aligned}0P_1&=\mathcal{O},\\ -P_1&=\overline{P_1}=(0,\alpha+1)=P_2,\\ 2P_1&=(1,\alpha)=P_3,\\ -2P_1&=\overline{2P_1}=(1,\alpha+1)=P_4,\\ 3P_1&=P_1+P_3=P_4=-2P_1,\end{aligned}$$

即有 $5P_1=\mathcal{O}$.

第 3 章 有限域上的椭圆曲线

在第 2 章中我们看到任意域上椭圆曲线的点构成一个群，由此就可以建立第 1 章中提及的公钥密码体制. 由点加计算公式可知，椭圆曲线上点之间的运算最终归结为基域中的运算，由此就必须确保基域中运算的有效性. 一般来说基域就只能取为有限域 (虽然有理数域和一般的数域上也可以完成精确的计算，但它们有两个缺点：首先元素可能会非常大，从而破坏计算的有效性. 更重要的是以此为基域的椭圆曲线上的离散对数问题是容易求解的). 由此在本章中，我们只考虑以下情形：

记 $k = \mathbb{F}_q$ 是 q 元有限域，其特征为素数 p, $K = \overline{k}$ 表示其代数闭包. E 是定义在 k 上的椭圆曲线，即椭圆曲线的系数 $a_1, a_3, a_2, a_4, a_6 \in k$. 和前面一样，我们依然用 E 表示椭圆曲线上所有坐标在 K 中的点所构成的群. 我们最感兴趣的是，椭圆曲线上所有坐标在 k 中的点 (称为 k 有理点) 所构成的群，记为 E_k. 由于 k 是一个有限域，则 E_k 中点的 X 坐标和 Y 坐标也只可能取有限个值，因此 E_k 就是一个有限交换群. 在第 4 章中我们将会看到，在 E_k 上建立的密码体制的安全性主要取决于 E_k 中元素的个数. 本章将花大部分的篇幅来证明著名的 Hasse 定理. 该定理对 E_k 的阶进行了估计，即

$$|q+1-|E_{\mathbb{F}_q}|| \leqslant 2\sqrt{q}.$$

由此可知 E_k 中的元素个数与 k 中元素个数是大体相当的.

这里我们仍然大体采用文献 [Charlap and Robbins, 1988] 的处理方式，偶尔地也会有所不同. 对于基域特征等于 2 的情形，我们也给出了相应定理的证明.

虽然本书前七节中得到的结果对于任意的有限和无限域都是成立的，但我们仅对有限域应用这些结论. 具体来说，就是用来证明 3.8 节中有关 Hasse 定理以及计算第 5 章中 E_k 的元素个数. 在本章的最后部分，我们讨论有限域上某些特殊的椭圆曲线并给出 E_k 的群结构.

3.1 有理映射和自同态

到目前为止，我们考虑的都是由椭圆曲线 E 到基域 k(或 K) 上的映射 —— 有理函数. 下面将定义 E 到自身上的映射. 对于仿射的情形，就是考察有理函数

对 $\alpha=(\alpha_1,\alpha_2)\in K(E)\times K(E)$，其满足：对于 E 上的任意一点 $P\in E$，$\alpha(P):=(\alpha_1(P),\alpha_2(P))$ 仍然是 E 上的点. 严格地说，就是

$$(E\circ\alpha)(P)=E(\alpha(P))=0,\quad \forall P\in E.$$

因此有理函数 $E(\alpha)=E\circ\alpha$ 就应当等于零，即如果把 E 看成是定义在域 $K(E)$ 上的椭圆曲线，则有理映射 $\alpha=(\alpha_1,\alpha_2)$ 是该椭圆曲线上的点. 为此我们有以下定义：

定义3.1　称椭圆曲线 $E_{K(E)}$ 上的点就是一个有理映射. 为避免混淆，我们记该曲线上的无穷远点为 $[0]$.

上面的定义可以直接推广到不同椭圆曲线 E,E' 之间的有理映射 (参见定义 5.12). 建议读者在一般意义下对以下结果的正确性加以验证.

对于有理映射，我们更多地考虑其仿射形式而不采用射影形式，为此就必须定义点 $P\in E$ 在有理映射 α 下的像. 首先对于零映射 $[0]$ 而言，其将曲线上的任意一点映为 E 上的无穷远点 $\mathcal{O}$. 否则记 $\alpha=(\alpha_1,\alpha_2)$. 如果 α_1,α_2 在 P 点处都是正则的，则令 $\alpha(P)=(\alpha_1(P),\alpha_2(P))$；如果 α_1,α_2 在 P 点处不正则，则令 $\alpha(P)=\mathcal{O}$. 要注意的是由于 α_1,α_2 满足

$$\alpha_2^2+a_1\alpha_1\alpha_2+a_3\alpha_2=\alpha_1^3+a_2\alpha_1^2+a_4\alpha_1+a_6,$$

因此 α_1,α_2 要么在 P 点处均正则，要么均不正则：若 $\mathrm{ord}_P\alpha_1<0$, $\mathrm{ord}_P\alpha_2\geqslant 0$, 则由命题 2.14 知左式在 P 点处的阶大于等于 $\mathrm{ord}_P\alpha_1$，而右式在 P 点处的阶 $3\mathrm{ord}_P\alpha_1<\mathrm{ord}_P\alpha_1$，矛盾. 当 $\mathrm{ord}_P\alpha_2<0,\mathrm{ord}_P\alpha_1\geqslant 0$ 时，也可类似地证明.

由于有理映射被定义成特殊椭圆曲线上的点，因此其在通常的加法运算下也构成群. 很自然地我们要考虑一个点在两个有理映射和的作用下的像. 对此下面的定理给出了解答. 该定理的符号很有启发性，但是证明要花很大的篇幅：

定理3.2　设 α,β 是两个有理映射，则

$$(\alpha+\beta)(P)=\alpha(P)+\beta(P),\quad \forall P\in E.$$

证明　为证明该定理，需要根据椭圆曲线上的运算规则分不同的情况加以讨论. 要注意的是等式两边中的加法运算是定义在不同域上椭圆曲线 (即 $E_{K(E)}$和E_K) 的点加运算. 同时即使 $\alpha\neq\pm\beta$，对于特殊的点 P，仍然可能有 $\alpha(P)=\pm\beta(P)$. 这样也就使证明变得比较复杂. 设 P 是 E 上的某个固定点.

- 当 α,β 中有一个等于 $[0]$ 时，定理显然成立.

  记 $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)$.
- 当 $\alpha=-\beta$ 时，有 $\alpha_1=\beta_1,\alpha_2=-\beta_2-a_1\beta_1-a_3$. 若 $\alpha_1=\beta_1$ 在 P 点处不正则，则有

$$\alpha(P)+\beta(P)=\mathcal{O}+\mathcal{O}=\mathcal{O}=[0](P)=(\alpha+\beta)(P);$$

  否则

$$\alpha_1(P)=\beta_1(P),\quad \alpha_2(P)=-\beta_2(P)-a_1\beta_1(P)-a_3,$$

  所以 $\alpha(P)=-\beta(P)$, 即 $\alpha(P)+\beta(P)=\mathcal{O}$, 因此定理成立.

在余下的情况中，有 $\alpha+\beta\neq[0]$，因此不妨记 $\alpha+\beta=\gamma=(\gamma_1,\gamma_2)$.

- 当 $\alpha\neq\beta$ 时，有

$$\gamma_1=-\alpha_1-\beta_1+\lambda^2+\lambda a_1-a_2, \tag{3.1}$$

$$\gamma_2=\lambda(\alpha_1-\gamma_1)-\beta_1-(a_1\gamma_1+a_3), \tag{3.2}$$

  其中

$$\lambda=\frac{\beta_2-\alpha_2}{\beta_1-\alpha_1}. \tag{3.3}$$

  对此再区分以下几种情况：

  —— 若 $\alpha(P)$, $\beta(P)$ 是不同的有限点，且 $\alpha(P)\neq-\beta(P)$，则将 P 代入等式 (3.1)~(3.3) 就可以得到 $\alpha(P)$, $\beta(P)$ 在加法运算下的计算公式，因此 $\gamma(P)=\alpha(P)+\beta(P)$.

  —— 若 $\alpha(P)$, $\beta(P)$ 是不同的有限点，且 $\alpha(P)=-\beta(P)$，则 $\alpha_1(P)=\beta_1(P),\alpha_2(P)\neq\beta_2(P)$，因此点 P 为 λ 的极点. 由命题 2.14 知，P 也是 γ_1 的极点，因此 $\gamma(P)=\mathcal{O}=\alpha(P)+\beta(P)$.

  —— 若 $\alpha(P)=\beta(P)$ 是有限点，且不为 2 阶点，即 $\alpha_1(P)=\beta_1(P)=:x$, $\alpha_2(P)=\beta_2(P)=:y$ 且 $2y+a_1x+a_3\neq0$. 由于在 $\alpha+\beta$ 和 $\alpha(P)+\beta(P)$ 的计算公式中唯一不同的就是 λ 的定义. 而对于后者中，我们有

$$\lambda'(P)=\frac{3\alpha_1^2+2a_2\alpha_1+a_4-a_1\alpha_2}{2\alpha_2+a_1\alpha_1+a_3}(P),$$

  因此只需证明 $\lambda(P)=\lambda'(P)$ 即可. 由于

$$\begin{aligned}\lambda&=\frac{\beta_2-\alpha_2}{\beta_1-\alpha_1}\\&=\frac{\beta_2-\alpha_2}{\beta_1-\alpha_1}\cdot\frac{\beta_2+\alpha_2+a_1\alpha_1+a_3}{\beta_2+\alpha_2+a_1\alpha_1+a_3}\end{aligned}$$

$$= \frac{(\beta_2^2 + a_1\beta_1\beta_2 + a_3\beta_2) - a_1\beta_2(\beta_1 - \alpha_1) - (\alpha_2^2 + a_1\alpha_1\alpha_2 + a_3\alpha_2)}{(\beta_1 - \alpha_1)(\beta_2 + \alpha_2 + a_1\alpha_1 + a_3)}$$
$$= \frac{(\beta_1^3 - \alpha_1^3) + a_2(\beta_1^2 - \alpha_1^2) + (a_4 - a_1\beta_2)(\beta_1 - \alpha_1)}{(\beta_1 - \alpha_1)(\beta_2 + \alpha_2 + a_1\alpha_1 + a_3)}$$
$$= \frac{(\beta_1^2 + \beta_1\alpha_1 + \alpha_1^2) + a_2(\beta_1 + \alpha_1) + (a_4 - a_1\beta_2)}{\beta_2 + \alpha_2 + a_1\alpha_1 + a_3},$$

其中第 4 个等号成立的原因是：由有理映射的定义知，α, β 必定满足方程 E. 又由于 $\alpha(P) = \beta(P) = (x, y)$，因此

$$\lambda(P) = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} = \lambda'(P).$$

—— 若 $\alpha(P) = \beta(P)$ 是有限 2 阶点，则正如前一种情况那样，有

$$\lambda = \frac{(\beta_1^2 + \beta_1\alpha_1 + \alpha_1^2) + a_2(\beta_1 + \alpha_1) + (a_4 - a_1\beta_2)}{\beta_2 + \alpha_2 + a_1\alpha_1 + a_3}.$$

因此在 P 点处上式分母、分子的值分别为 $\frac{\partial E}{\partial Y}(\alpha(P))$ 以及 $-\frac{\partial E}{\partial X}(\alpha(P))$. 由于 $\alpha(P)$ 为 2 阶点，因此 $\frac{\partial E}{\partial Y}(\alpha(P)) = 0$. 又由于 E 是非奇异的，所以 $\frac{\partial E}{\partial X}(\alpha(P)) \neq 0$. 由此可知 P 为 λ 的极点，因此由命题 2.14 知 γ 也以 P 为极点，从而 $\gamma(P) = \mathcal{O} = 2\alpha(P)$.

—— 若 $\alpha(P), \beta(P)$ 中恰有一个是无穷远点，不妨设 $\alpha(P) = \mathcal{O}$，则 $\alpha_1 = u^{d_1}\alpha_1'$，$\alpha_2 = u^{d_2}\alpha_2'$，其中 u 是 P 点处的一致化参数且 $d_1, d_2 < 0$，而 α_1', α_2' 在 P 点处正则且不等于零. 我们第一个目标是证明 $\gamma(P)$ 是有限点. 由 $E(\alpha_1, \alpha_2) = 0$ 及命题 2.14 可得

$$\begin{aligned}\min\{2d_2, d_1 + d_2\} &\leqslant \mathrm{ord}_P(\alpha_2^2 + a_1\alpha_1\alpha_2 + a_3\alpha_2) \\ &= \mathrm{ord}_P(\alpha_1^3 + a_2\alpha_1^2 + a_4\alpha_1 + a_6) \\ &= 3d_1,\end{aligned}$$

由此及 $d_1, d_2 < 0$ 可知 $d_2 < d_1$，因此由命题 2.14 可知 $2d_2 = 3d_1$. 将 (3.3) 代入 (3.1)，并用 $\alpha_1^3 + a_2\alpha_1^2 + a_4\alpha_1 + a_6 - a_1\alpha_1\alpha_2 - a_3\alpha_2$ 代替 α_2^2(对于 β_2^2 也类似处理)，则有

$$\begin{aligned}\gamma_1 =& \frac{(\alpha_1\beta_1 + a_4)(\alpha_1 + \beta_1) - a_1(\alpha_1\beta_2 + \beta_1\alpha_2) + 2a_2\alpha_1\beta_1}{(\alpha_1 - \beta_1)^2} \\ &- \frac{a_3(\alpha_2 + \beta_2) + 2\alpha_2\beta_2 - 2a_6}{(\alpha_1 - \beta_1)^2}.\end{aligned}$$

由于 $\mathrm{ord}_P(\beta_1)$, $\mathrm{ord}_P\beta_2 \geqslant 0$, 因此由命题 2.14 知

$$\mathrm{ord}_P\gamma_1 \geqslant \min\{2d_1, d_2\} - 2d_1 = \min\{0, d_2 - 2d_1\} = \min\left\{0, -\frac{1}{2}d_1\right\} = 0.$$

考虑到有理映射的群运算满足结合律和交换律, 则可记 $\alpha = \gamma - \beta$, 其中 γ 和 β 在 P 点都是有限的. 由已经证明的情况可知 $\alpha(P) = \gamma(P) - \beta(P)$.
—— 若 $\alpha(P) = \beta(P) = \mathcal{O}$, 假设 $\gamma(P) \neq \mathcal{O}$, 则由已经证明的情况及 $\alpha = \gamma - \beta$ 知 $\mathcal{O} = \alpha(P) = \gamma(P) - \beta(P) = \gamma(P)$, 矛盾.

- 当 $\alpha = \beta \neq -\beta$ 时, 则有 γ_1 满足 (3.1), 其中

$$\lambda = \frac{3\alpha_1^2 + 2a_2\alpha_1 + a_4 - a_1\alpha_2}{2\alpha_2 + a_1\alpha_1 + a_3}.$$

对此区分以下两种情况:

—— 若 $\alpha(P) \neq \mathcal{O}$, 则将 P 代入 (3.1) 即可得 $\gamma(P) = 2\alpha(P)$, 其恰好就是 E 上的倍点公式.

—— 若 $\alpha(P) = \mathcal{O}$, 假设 $\gamma(P) \neq \mathcal{O}$, 则由 $\alpha = \gamma - \alpha$ 以及已经证明的情况可知 $\mathcal{O} = \gamma(P)$, 矛盾. □

例 显然恒等映射 $\mathrm{id} = (X, Y)$ 以及常值映射 $c_Q = (x, y)$ 是两个有理映射, 其中 $Q = (x, y) \in E$. 由此可构造出一个更重要的映射 —— 关于 Q 点的平移映射:

$$\tau_Q : P \mapsto P + Q.$$

定理 3.2 表明由点定义的映射 τ_Q 可表示为

$$\tau_Q = \mathrm{id} + c_Q.$$

由于右式是一个有理函数, 因此 τ_Q 也是一个有理映射.

命题3.3 *有理映射要么是满射, 要么是一个常值映射.*

证明 首先我们对有理函数给出一个类似的结论. 设 r 是一个非常值的有理函数, 则 r 必定有一个零点. 同样地有理函数 $r - x$ 也必定存在零点, 其中 $x \in K$, 因此 r 取遍 K 中所有的值.

下面考虑有理映射 $\alpha = (\alpha_1, \alpha_2)$. 如果 α_1 是一个常数, 则 α_2 只能取有限个值, 即 $E(\alpha_1, Y) \in K[Y]$ 在 K 中的根, 因此 α_2 一定不是满射, 从而由上知其必为常数, 所以 α 必定是一个常值映射. 对于有理函数 α_1, 当其不是常数时, 由上知其必定是一个满射, 因此其必定有一个零点. 由定理 2.28 知其也必定有一个极点, 所以有

理映射 α 必能够取到 $\mathcal{O}$. 对于任意的 $Q \in E$, 考虑 $\tau_{-Q} \circ \alpha$, 则类似地可知必定存在点 $P \in E$ 使得

$$(\tau_{-Q} \circ \alpha)(P) = \tau_{-Q}(\alpha(P)) = \alpha(P) - Q = \mathcal{O},$$

因此 $\alpha(P) = Q$. □

定义3.4　如果某个有理映射是一个群同态, 则称其为自同态或同种映射. E 上自同态的全体记为 $\mathrm{End}(E)$.

命题3.5　$\mathrm{End}(E)$ 是一个环, 其乘法为映射的合成.

证明　显然只需证明其满足分配律即可. 设 α, β, γ 是三个自同态, 则有

$$\begin{aligned}(\alpha \circ (\beta + \gamma))(P) &= \alpha((\beta + \gamma)(P)) \\ &= \alpha(\beta(P) + \gamma(P)) \quad (\text{定理 } 3.2) \\ &= \alpha(\beta(P)) + \alpha(\gamma(P)) \quad (\alpha\text{是一个同态}) \\ &= (\alpha \circ \beta)(P) + (\alpha \circ \gamma)(P).\end{aligned}$$

因此

$$\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma.$$

同样地也容易证明 $(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$. □

例　对于前一例题中考虑的常值映射以及平移映射, 显然其中只有 $c_{\mathcal{O}} = [0]$, $\tau_{\mathcal{O}} = \mathrm{id}$ 才为自同态. 我们更感兴趣的是下面的 m 乘映射:

$$[m] : P \mapsto mP,$$

其中 $m \in \mathbb{Z}$. 由定理 3.2 知

$$mP = \begin{cases} (m-1)P + P, & m > 0, \\ -((-m)P), & m < 0, \end{cases}$$

对应着

$$[m] = \begin{cases} [m-1] + \mathrm{id}, & m > 0, \\ -[-m], & m < 0. \end{cases}$$

因此我们可以递归地看到 $[m]$ 是一个有理映射. 同时又由于 $m(P+Q) = mP + mQ$, 因此其是一个自同态.

推论3.6 End(E) 是一个 $\mathbb{Z}$ 代数，其中 $m \in \mathbb{Z}$ 在 End(E) 元素上的作用被定义为其与 $[m]$ 的合成.

证明 在命题 3.5 中我们已经证明了 End(E) 是一个环，则由以上关于 m 乘映射的例子可知，$\mathbb{Z}$ 是 End (E) 的子环，因此 End (E) 作为 $\mathbb{Z}$ 模来说，就构成 $\mathbb{Z}$ 代数. □

定义3.7 如果 End(E) 中除 $[m]$ 以外，还存在其他自同态，则称 E 有复乘.

若 $k = \mathbb{F}_q$ 是一个有限域，则 E 必定存在复乘，即所谓的 Frobenius 自同态 $\varphi = (X^q, Y^q)$：若 $P = (x, y)$ 是 E 上的点，则 $E(\varphi(P)) = E(x^q, y^q) = E(x, y)^q = 0$，因此 $\varphi(P) \in E$. 注意在说明 $E(x^q, y^q) = E(x, y)^q$ 时，我们利用了 "E 是定义在 k 上的椭圆曲线" 这一条件，因此对于系数有 $a_i^q = a_i$. 由于 φ 与有理映射的加法公式是相容的，由此可知 φ 的确是一个自同态. Frobenius 自同态是证明 Hasse 定理的重要工具. 同时将具有 $\mathbb{Z}$ 模结构的自同态环 End(E) 作用到 m 扭点也是证明该定理的重要方法，而这一方法与 m 乘映射是密切相关的.

定义3.8 设 m 是一个整数，$P \in E$，若 $mP = \mathcal{O}$，则称 P 是一个 m 扭点. 记 $E[m]$ 表示全体 m 扭点构成的集合. 如果 $mP = \mathcal{O}$ 且对于任意的 m'，$0 < m' < m$，有 $m'P \neq \mathcal{O}$，则称 m 为 P 点的阶.

注意 m 扭点就构成了自同态 $[m]$ 的核.

定理3.9 设 m 是一个非零整数，则 $E[m]$ 是有限集合且 $[m] \neq [0]$. 由此可记 $[m] = (g_m, h_m)$. 有理函数 g_m, h_m 恰好以 $E[m]$ 中的点为极点.

证明 首先说明 $[m] \neq [0]$ 等价于 $|E[m]| < \infty$：若 $[m] = [0]$，则 $E[m] = \ker[m] = E$ 是无限集合；若 $[m] = (g_m, h_m) \neq [0]$，则 $[m]P = mP = \mathcal{O}$ 意味着 g_m, h_m 以 P 点为极点. 由于有理函数只有有限个极点，因此 $E[m]$ 必定有限. 下面只需要证明 $[m] \neq [0]$ 即可. 由于 $E[-m] = E[m]$，因此只需考虑 m 为正数的情况. 为此我们分以下几种情况加以讨论：

1. 当 $m = 1$ 时，定理显然成立.
2. 当 $m = 2$ 时，此时就是要说明 $[2] \neq [0]$，即 $[1] \neq [-1]$. 这点也是显然的.
3. 当 m 是一奇素数且 $p \neq 2$ 时，由 2.5 节知此时存在 2 阶点 P，因此有

$$mP = (m-1)P + P = \mathcal{O} + P = P \neq \mathcal{O},$$

由此可知 $[m] \neq [0]$.

4. 当 m 是一奇素数且 $p=2$ 时，若 $j\neq 0$，则由 2.5 节知存在 2 阶点，因此由以上的证明同样可得 $[m]\neq[0]$. 若 $j=0$，我们说明此时必定存在 3 阶点，然后再用同样的方法加以证明. 由 2.3 节知，此时不妨设 $E: Y^2+a_3Y=X^3+a_4X+a_6$. 由 $P=(x,y)$ 的倍点计算公式可知

$$X(2P)=\frac{x^4+a_4^2}{a_3^2}$$

且

$$X(-P)=X(P).$$

由于 3 扭点 P 恰好满足 $2P=\pm P$，即 $X(2P)=X(P)$，为此取 $x\in K$ 满足 $\frac{x^4+a_4^2}{a_3^2}=x$ 并通过在 K 中求解方程 $E(x,Y)=0$ 确定点 $P=(x,y)$，则 P 就是一个 3 阶点. 如果 $m\neq 3$，则 $mP\neq\mathcal{O}$，进而有 $[m]\neq[0]$. 最后注意到

$$E[3]=\{(x,y): x^4+a_3^2x+a_4^2=0, E(x,y)=0\}$$

必定是一个有限集合：x 可能的取值至多只有 4 个，而每个 x 至多对应着 2 个可能的 y 值，因此 $[3]\neq[0]$.

5. 当 m 是一个合数时，我们对其素因子个数进行归纳. 设 d 是 m 的一个真因子，则由归纳假设知，群同态

$$\rho: E[m]\to E[d],\quad P\mapsto \frac{m}{d}P$$

的像是 $E[d]$ 的一个有限子群，其核 $E\left[\frac{m}{d}\right]$ 也是一个有限子群. 由此可知 $|E[m]|=|\operatorname{Im}\rho||\ker\rho|$ 也是有限的，因此 $[m]\neq[0]$. □

推论3.10　*若 $m\neq n$，则 $[m]\neq[n]$.*

证明　若 $[m]=[n]$，则 $[m-n]=[0]$. 因此由定理 3.9 知 $m-n=0$. □

由于 $g_1=X$，$h_1=Y$，则利用推论 3.10 就可以依次计算出 g_m，h_m. 为计算 g_2，h_2，由 $[2]=[1]+[1]$ 以及倍点计算公式可得：

$$g_2=-2X+\lambda^2+a_1\lambda-a_2,$$

$$h_2=-\lambda(g_2-X)-a_1g_2-a_3-Y,$$

$$\lambda=\frac{3X^2+2a_2X+a_4-a_1Y}{2Y+a_1X+a_3}.$$

若 $m > 2$，则由推论 3.10 知 $[m-1] \neq [1]$，因此由点加计算公式则可计算 $[m] = [m-1] + [1]$ 如下：

$$\begin{aligned} g_m &= -g_{m-1} - X + \lambda^2 + a_1\lambda - a_2, \\ h_m &= -\lambda(g_m - X) - a_1 g_m - a_3 - Y, \\ \lambda &= \frac{h_{m-1} - Y}{g_{m-1} - X}. \end{aligned}$$

3.2 分歧指数与次数

设 $\alpha = (\alpha_1, \alpha_2)$ 是一个有理映射，对任意的 $r(X,Y) \in k(E)$，有 $r \circ \alpha = r(\alpha_1, \alpha_2) \in k(E)$. 在本节中我们考虑由 α 所诱导出的映射

$$\alpha^* : K(E) \to K(E), \quad r \mapsto r \circ \alpha.$$

第一个结论来自于命题 3.3.

命题3.11 *如果 α 是一个非常值的有理映射，则 α^* 是一个域单同态.*

证明 显然 α^* 是域同态. 如果 $r \circ \alpha = s \circ \alpha$，则对于任意的 $P \in E$，有 $r(\alpha(P)) = s(\alpha(P))$. 由推论 3.3 知 α 必定是一个满射，即 $\alpha(P)$ 取遍 E 上所有的点，因此对任意的 $Q \in E$，有 $r(Q) = s(Q)$，即 $r = s$. □

对于点 P，设 u 为 $\alpha(P)$ 处的一致化参数. 由于 u 在 $\alpha(P)$ 处的阶等于 1，读者可能会以为 $u \circ \alpha$ 在 P 处的阶也等于 1，但实际情况并非如此. 对此有以下定义：

定义3.12 *设 α 是一个非常值的有理映射，$P \in E$ 而 u 是 $\alpha(P)$ 处的一致化参数，则称*

$$e_\alpha(P) := \mathrm{ord}_P(u \circ \alpha)$$

是 α 在 P 点处的分歧指数. 如果 $e_\alpha > 1$，则称 α 在 P 点处是分歧的，否则称其在 P 点处非分歧. 如果 α 在 E 的所有点处都是非分歧的，则称 α 是非分歧的.

注意分歧指数与一致化参数 u 的选取是无关的. 设 u' 是 $\alpha(P)$ 处另一个一致化参数，则 $\frac{u'}{u}$ 在 $\alpha(P)$ 处是正则的且不等于零，因此 $\frac{u'}{u} \circ \alpha$ 在 P 点处仍是正则的且不为零，所以有

$$\mathrm{ord}_P(u' \circ \alpha) = \mathrm{ord}_P\left(\left(u\frac{u'}{u}\right) \circ \alpha\right)$$

$$= \mathrm{ord}_P(u \circ \alpha) + \mathrm{ord}_P\left(\frac{u'}{u} \circ \alpha\right)$$
$$= \mathrm{ord}_P(u \circ \alpha).$$

我们期望由 α 诱导出除子群 $\mathrm{Div}(E)$ 之间的映射 α^*，使得该映射与上面诱导出的函数域 $K(E)$ 之间的映射 α^* 是 “相同” 的，即得到的 α^* 与主除子是可交换的. 下面的命题 3.13 表明，如下定义的映射满足这样的要求：

$$\alpha^* : \mathrm{Div}(E) \to \mathrm{Div}(E), \quad \langle Q \rangle \mapsto \sum_{P \in \alpha^{-1}(Q)} e_\alpha(P)\langle P \rangle$$

并将其 $\mathbb{Z}$ 线性扩展到整个 $\mathrm{Div}(E)$ 上，即如果

$$D = \sum_Q n_Q \langle Q \rangle \in \mathrm{Div}(E),$$

则有

$$\alpha^*(D) = \sum_Q n_Q \alpha^* \langle Q \rangle.$$

命题3.13　对于非常值的有理映射 α，下图是交换的

$$\begin{array}{ccc} K(E) & \xrightarrow{\alpha^*} & K(E) \\ \downarrow{\scriptstyle \mathrm{div}} & & \downarrow{\scriptstyle \mathrm{div}} \\ \mathrm{Div}(E) & \xrightarrow{\alpha^*} & \mathrm{Div}(E) \end{array} \qquad \begin{array}{ccc} r & \longrightarrow & r \circ \alpha \\ \downarrow & & \downarrow \\ \mathrm{div}\, r & \longrightarrow & \mathrm{div}(r \circ \alpha) \end{array}$$

引理3.14　设 α 是非常值的有理映射，r 为有理函数，$P \in E$，则

$$\mathrm{ord}_P(r \circ \alpha) = e_\alpha(P)\mathrm{ord}_{\alpha(P)}(r).$$

证明　设 u 是 $\alpha(P)$ 处的一致化参数. 当 $r = u$ 时，由分歧指数的定义知引理是显然成立的. 记 $r = u^d r_1$，其中有理函数 r_1 在 $\alpha(P)$ 处正则且不等于零，则

$$\mathrm{ord}_P(r \circ \alpha) = d\, \mathrm{ord}_P(u \circ \alpha) + \mathrm{ord}_P(r_1 \circ \alpha)$$
$$= d\, e_\alpha(P).$$

□

命题 3.13 的证明

$$\mathrm{div}(r \circ \alpha) = \sum_{P \in E} \mathrm{ord}_P(r \circ \alpha)\langle P \rangle$$

$$
\begin{aligned}
&= \sum_{P\in E} e_\alpha(P)\mathrm{ord}_{\alpha(P)}(r)\langle P\rangle \qquad (\text{引理 } 3.14)\\
&= \sum_{Q\in E} \mathrm{ord}_Q(r) \sum_{P\in\alpha^{-1}(Q)} e_\alpha(P)\langle P\rangle\\
&= \sum_{Q\in E} \mathrm{ord}_Q(r)\alpha^*(\langle Q\rangle) \qquad (\alpha^* \text{ 的定义})\\
&= \alpha^*\left(\sum_{Q\in E}\mathrm{ord}_Q(r)\langle Q\rangle\right)\\
&= \alpha^*(\mathrm{div}\, r).
\end{aligned}
$$

□

为了后面的计算，我们需要考虑两个有理映射的复合：

命题3.15 设 α,β 是非常值的有理映射，则 $\beta\circ\alpha$ 也是非常值的，且有

$$
\begin{aligned}
&e_{\beta\circ\alpha}(P) = e_\alpha(P)e_\beta(\alpha(P)), \quad \forall P\in E,\\
&(\beta\circ\alpha)^* = \alpha^*\circ\beta^*.
\end{aligned}
$$

证明 由于 α,β 都是满射，因此 $\beta\circ\alpha$ 也是满射，从而 $\beta\circ\alpha$ 是非常值的. 设 u 是 $(\beta\circ\alpha)(P)$ 处的一致化参数，则

$$
\begin{aligned}
e_{\beta\circ\alpha}(P) &= \mathrm{ord}_P((u\circ\beta)\circ\alpha)\\
&= e_\alpha(P)\mathrm{ord}_{\alpha(P)}(u\circ\beta) \qquad (\text{引理 } 3.14)\\
&= e_\alpha(P)e_\beta(\alpha(P)), \qquad (\text{引理 } 3.14)
\end{aligned}
$$

因此第一个等式成立.

$$
\begin{aligned}
(\beta\circ\alpha)^*(\langle Q\rangle) &= \sum_{P\in(\beta\circ\alpha)^{-1}(Q)} e_{\beta\circ\alpha}(P)\langle P\rangle\\
&= \sum_{P\in(\beta\circ\alpha)^{-1}(Q)} e_\beta(\alpha(P))e_\alpha(P)\langle P\rangle\\
&= \sum_{R\in\beta^{-1}(Q)} e_\beta(R) \sum_{P\in\alpha^{-1}(R)} e_\alpha(P)\langle P\rangle\\
&= \sum_{R\in\beta^{-1}(Q)} e_\beta(R)\alpha^*(\langle R\rangle)\\
&= \alpha^*\left(\sum_{R\in\beta^{-1}(Q)} e_\beta(R)\langle R\rangle\right)\\
&= \alpha^*\circ\beta^*(\langle Q\rangle),
\end{aligned}
$$

所以第二个等式也成立. □

下面以平移映射作为第一个例子.

引理3.16　设 $Q \in E$, 则映射 τ_Q 是非分歧的.

证明　由于 τ_Q 有逆有理映射 τ_{-Q}, 因此

$$1 = e_{\mathrm{id}}(P) = e_{\tau_{-Q} \circ \tau_Q}(P) = e_{\tau_Q}(P) e_{\tau_{-Q}}(P+Q).$$

而由于 $e_{\tau_Q}(P)$ 和 $e_{\tau_{-Q}}(P+Q)$ 都至少是 1, 因此 $e_{\tau_Q}(P) = 1$. □

以上关于平移映射的结论可用于证明下面关于自同态的结论 —— 定理 3.17. 由此可见自同态的分歧性是比较简单的.

定理3.17　设 α 是一个非零自同态, 则 $e_\alpha = e_\alpha(P)$ 与点 P 无关.

证明　设 P 是 E 上的点. 由于对于任意的 $Q \in E$, 有 $\alpha(Q+P) = \alpha(Q) + \alpha(P)$, 因此 $\alpha \circ \tau_P = \tau_{\alpha(P)} \circ \alpha$, 则

$$\begin{aligned}
e_\alpha(P) &= \frac{e_{\alpha \circ \tau_P}(\mathcal{O})}{e_{\tau_P}(\mathcal{O})} \quad (\text{命题 } 3.15) \\
&= e_{\alpha \circ \tau_P}(\mathcal{O}) \quad (\text{引理 } 3.16) \\
&= e_{\tau_{\alpha(P)} \circ \alpha}(\mathcal{O}) \\
&= e_\alpha(\mathcal{O}) e_{\tau_{\alpha(P)}}(\alpha(\mathcal{O})) \\
&= e_\alpha(\mathcal{O}).
\end{aligned}$$

□

推论3.18　设 α, β 是非零自同态, 则

$$e_{\beta \circ \alpha} = e_\alpha e_\beta.$$

证明　由定理 3.17 及命题 3.15 可知该推论是显然的. □

作为第一个非平凡的例子, 我们考察 $k = \mathbb{F}_q$ 上的 Frobenius 自同态 φ:

命题3.19

$$e_\varphi = q$$

证明　由 2.7 节知 $\dfrac{X}{Y}$ 是 $\mathcal{O} = \varphi(\mathcal{O})$ 处的一致化参数, 因此

$$e_\varphi = e_\varphi(\mathcal{O}) = \mathrm{ord}_{\mathcal{O}}\left(\frac{X}{Y} \circ \varphi\right) = \mathrm{ord}_{\mathcal{O}}\left(\left(\frac{X}{Y}\right)^q\right) = q.$$

□

本节中需要引入的第二个概念是自同态 α 的次数. 由于 α^* 的像实际上是 $K(E)$ 的一个子域, 因此很自然地, $\deg\alpha$ 就被定义为域扩张 $K(E)/\alpha^*(K(E))$ 的次数. 由于 $K(E),\alpha^*(K(E))$ 都是 K 的超越次数等于 1 的扩域且 $[K(E):K(X)]<\infty$, 因此 $\deg\alpha$ 必定是有限的. 可以证明 $\deg\alpha=e_\alpha|\ker\alpha|$(参见 [Shafarevich, 1974], p.141–143), 该结论的证明与数域中有关扩域的扩张次数与分歧指数及惯性指数关系的定理证明是类似的. 更进一步地, e_α、$|\ker\alpha|$ 分别是域扩张 $K(E)/\alpha^*(K(E))$ 的纯不可分次数和可分次数. 由于该结论的证明牵涉到许多理论知识, 在此我们将该结论作为定义, 但这样处理的缺点是会遗漏许多重要的信息, 同时使得在本书中难以使用该次数.

定义3.20 定义非零自同态 α 的次数为

$$\deg\alpha=e_\alpha|\ker\alpha|.$$

例 在命题 3.19 中我们已经知道 $e_\varphi=q$. 又由于对于有限点 $P=(x,y)$, 其像点 $\varphi(P)=(x^q,y^q)$ 也是有限点, 因此 $\ker\varphi=\{\mathcal{O}\}$, 从而有 $\deg\varphi=q$. 记 $J=\varphi^*(K(E))$, 我们考察扩域 $K(E)/J$. 由于 $K(E)$ 是在 K 上添加 X, Y 得到的扩域且 φ^* 在 K 上为恒等映射, 因此 J 是在 K 上添加 X^q, Y^q 得到的扩域, 所以其是 $K[X^q,Y^q]/(E)$ 的分式域, 则有 $K(E)=J(X,Y)$. 当 $p\neq 2$ 时, 不妨设 E 为标准形式 $Y^2=X^3+a_2X^2+a_4X+a_6$, 因此

$$Y=\frac{(Y^2)^{\frac{q+1}{2}}}{Y^q}=\frac{(X^3+a_2X^2+a_4X+a_6)^{\frac{q+1}{2}}}{Y^q}\in J(X),$$

则有 $K(E)=J(X)$. 若 $q=2^m$, 则

$$Y=\frac{X^3+a_2X^2+a_4X+a_6+Y^2}{a_1X+a_3}\in J(X,Y^2),$$

因此有

$$K(E)=J(X,Y)=J(X,Y^2)=J(X,Y^4)=\cdots=J(X,Y^q)=J(X).$$

由于 X 是不可约多项式 $T^q-X^q\in J[T]$ 的根, 因此 $[K(E):J]$ 就等于 $q=\deg\varphi$. 更进一步地, 由于该多项式是不可分的, 因此 $K(E)/J$ 是纯不可分的, 这点就对应着已知的 $|\ker\varphi|=1$.

命题3.21 设 $\Delta\in\mathrm{Div}(E)$, α, β 是非零自同态, 则

1. $\deg(\alpha^*(\Delta))=\deg\alpha\ \deg\Delta$,
2. $\deg(\alpha\circ\beta)=\deg\alpha\ \deg\beta$.

证明

1. 由次数函数在除子上的线性性以及 α^* 的线性性知，只需考虑 $\Delta = \langle Q \rangle$ 即可.

$$\begin{aligned}\deg(\alpha^*(\Delta)) &= \deg\left(e_\alpha \sum_{P \in \alpha^{-1}(Q)} \langle P \rangle\right) \\ &= e_\alpha |\alpha^{-1}(Q)| \\ &= e_\alpha |\ker \alpha| \\ &= \deg \alpha.\end{aligned}$$

2.

$$\begin{aligned}\deg(\alpha \circ \beta) &= e_{\alpha\circ\beta} |\ker(\alpha \circ \beta)| \\ &= e_\alpha e_\beta |\{P \in E : \beta(P) \in \ker \alpha\}| \quad (\text{推论 } 3.18) \\ &= e_\alpha e_\beta |\ker \alpha| |\ker \beta| = \deg \alpha \ \deg \beta.\end{aligned}$$

□

我们的目标是研究映射 $[m]$ 以及 m 扭点 $E[m]$. 特别地我们对 $[m]$ 的分歧指数 $e_{[m]}$ 很感兴趣. 为此我们需要一些预备知识，具体内容详见以下几节.

3.3　$K(E)$ 上的导数

本节中我们要定义 $K(E)$ 上的导数. 它与通常意义下 $K(X)$ 上的导数起着类似的作用，可用于判断有理函数零点的重数.

定义3.22　设 L 是一个 K 代数. L 上的导数就是一个 K 线性映射 $D: L \to L$, 其满足乘法规则

$$D(fg) = fDg + gDf.$$

对 $f = g = 1$ 应用乘法规则可得 $D1 = 2D1$, 因此 $D1 = 0$, 从而对于常数 $c \in K$, 有 $Dc = cD1 = 0$. 若 g 是 L 中的单位，记 $f = \dfrac{1}{g}$, 则有

$$0 = D\left(g\frac{1}{g}\right) = gD\frac{1}{g} + \frac{Dg}{g},$$

因此

$$D\frac{1}{g} = -\frac{Dg}{g^2}.$$

同样地对 $D\left(f\frac{1}{g}\right)$ 应用乘法规则，就可得下面的除法规则

$$D\frac{f}{g}=\frac{gDf-fDg}{g^2}.$$

由此可知 cf, $f\pm g$, fg, $\frac{f}{g}$ 的导数由 Df, Dg 唯一确定，其中 $f\in L$, $g\in L^{\times}$, $c\in K$.

首先我们确定 $K(X,Y)$ 上所有可能的导数.

命题3.23 设 $f,g\in K(X,Y)$，则在 $K(X,Y)$ 上存在唯一的导数 D，满足 $DX=f$, $DY=g$. 具体而言，即对于 $r\in K(X,Y)$

$$Dr=\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix}f\\g\end{pmatrix}.$$

证明 首先考虑唯一性. 由于 $K[X,Y]$ 是由 X, Y 生成的 K 代数，因此 DX, DY 的值确定了 $K[X,Y]$ 上的导数 D，因此由除法规则可知导数 D 可唯一地扩展到 $K(X,Y)$ 上.

从理论上看，具有指定 DX, DY 值的导数 D 的存在性是源于 X, Y 在 K 上的代数独立性. 为具体构造导数，我们考虑 K 线性函数

$$D':K(X,Y)\to K(X,Y),\quad r\mapsto\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix}f\\g\end{pmatrix},$$

则 D' 就是 $K(X,Y)$ 上的导数：由偏导数的线性性以及其乘法规则就直接可以得到 D' 的线性性及其乘法规则. 同时又有 $D'X=f$, $D'Y=g$，因此存在性成立. □

当在 $K[X,Y]/(E)$ 的分式域 $K(E)$ 上定义导数时，必须确保 $DE=D0=0$. 为此我们并不能任意选取 DX, DY，而是要求 DY 与 DX 是相互联系的.

命题3.24 对于 $f\in K(E)$，在 $K(E)$ 上存在唯一的导数 D 满足 $DX=f$. 具体而言，即

$$DY=\frac{3X^2+2a_2X+a_4-a_1Y}{2Y+a_1X+a_3}DX$$

且对于 $r\in K(E)$ 有

$$Dr=\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix}DX\\DY\end{pmatrix}.$$

证明 对于唯一性来说，注意到在 $K(E)$ 中有 $0=E$，而由乘法规则可得

$$0=DE=(2Y+a_1X+a_3)DY-(3X^2+2a_2X+a_4-a_1Y)DX,$$

因此 DY 是由 DX 所唯一确定的. 由于 $K[E]$ 是由 X, Y 生成的, 因此由命题 3.23 知将 D 扩展到 $K[E]$ 上的方式至多只有一种. 再由除法规则知其也就确定了 $K(E)$ 上的导数 D.

为证明存在性, 考虑函数

$$D : K(E) \to K(E), \quad r \mapsto \left(\frac{\partial r}{\partial X}, \frac{\partial r}{\partial Y}\right)\begin{pmatrix} DX \\ DY \end{pmatrix},$$

其中 DX, DY 如命题所示. 由此可得 $DE = 0$, 因此在 $K(E)$ 上 D 的定义是合理的. 再由直接计算就可以证明 D 的确是一个导数. □

以上的两个命题可以很容易地推广到一般的函数域: 设 L 是 K 上超越次数等于 n 的函数域, 即存在代数独立的元素 $X_1, \cdots, X_n \in L$, 使得 $L/K(X_1, \cdots, X_n)$ 是可分的. 由此知对于 $f_1, \cdots, f_n \in L$, 在 L 上存在唯一的导数 D, 满足 $DX_i = f_i$, $1 \leqslant i \leqslant n$.

$K(E)$ 上的导数与偏导数之间的关系可被用于研究有理函数与有理映射复合的导数.

命题3.25　设 $\alpha = (\alpha_1, \alpha_2)$ 是一个有理映射, r 是一个有理函数, 则

$$D(r \circ \alpha) = \left(\frac{\partial r}{\partial X} \circ \alpha, \frac{\partial r}{\partial Y} \circ \alpha\right)\begin{pmatrix} \dfrac{\partial \alpha_1}{\partial X} & \dfrac{\partial \alpha_1}{\partial Y} \\ \dfrac{\partial \alpha_2}{\partial X} & \dfrac{\partial \alpha_2}{\partial Y} \end{pmatrix}\begin{pmatrix} DX \\ DY \end{pmatrix}.$$

证明　由命题 3.24 以及 $r \circ \alpha$ 偏导数的链式法则, 该命题是很容易得到的. □

利用命题 3.24, 对于 DX 有一个很自然的选择, 满足 $DY \in K[E]$, 从而使 D 在 $K[E]$ 上的限制也是一个导数.

定义3.26　称以下的导数为 $K(E)$ 上的典范导数:

$$\begin{aligned} DX &= 2Y + a_1X + a_3 = \frac{\partial E}{\partial Y}, \\ DY &= 3X^2 + 2a_2X + a_4 - a_1Y = -\frac{\partial E}{\partial X}, \\ Dr &= \left(\frac{\partial r}{\partial X}, \frac{\partial r}{\partial Y}\right)\begin{pmatrix} DX \\ DY \end{pmatrix}, \quad r \in K(E). \end{aligned}$$

以下在本节中我们都讨论典范导数. 作为一个重要的实例, 我们计算 g_m, h_m 的导数.

定理3.27　设 m 是一个正整数, 则有

$$\begin{aligned}
Dg_m &= m(2h_m + a_1 g_m + a_3) \\
&= m\frac{\partial E}{\partial Y} \circ [m], \\
Dh_m &= m(3g_m^2 + 2a_2 g_m + a_4 - a_1 h_m) \\
&= -m\frac{\partial E}{\partial X} \circ [m].
\end{aligned}$$

证明 我们对 m 进行归纳，并单独处理 $m=1$, $m=2$ 时的情况. 由于整个计算过程是比较繁琐的，在此我们并没有给出所有的细节. 建议读者可在符号代数软件的帮助下仔细检查每个结果的正确性.

当 $m=1$ 时，定理的结果就是 DX, DY 的定义.

当 $m=2$ 时，利用倍点计算公式可得

$$DX = 2Y + a_1 X + a_3, \quad DY = 3X^2 + 2a_2 X + a_4 - a_1 Y, \tag{3.4}$$

$$\lambda = \frac{3X^2 + 2a_2 X + a_4 - a_1 Y}{2Y + a_1 X + a_3}, \tag{3.5}$$

$$g_2 = -2X + \lambda^2 + a_1 \lambda - a_2, \tag{3.6}$$

$$h_2 = -(\lambda + a_1) g_2 - a_3 - Y + \lambda X. \tag{3.7}$$

由此可得

$$\begin{aligned}
D\lambda =& \frac{((6X + 2a_2)DX - a_1 DY)(2Y + a_1 X + a_3)}{(2Y + a_1 X + a_3)^2} \\
& - \frac{(3X^2 + 2a_2 X + a_4 - a_1 Y)(2DY + a_1 DX)}{(2Y + a_1 X + a_3)^2},
\end{aligned} \tag{3.8}$$

$$Dg_2 = -2DX + 2\lambda D\lambda + a_1 D\lambda, \tag{3.9}$$

$$Dh_2 = -(\lambda + a_1) Dg_2 - g_2 D\lambda - DY + \lambda DX + X D\lambda. \tag{3.10}$$

将 (3.4) 中的 DX, DY 代入 (3.8)~(3.10) 式，再将 $D\lambda$ 代入 (3.9) 及 (3.10) 式，并再将得到的 Dg_2 代入 (3.10)，就可将 Dg_2, Dh_2 表示为 X, Y 的有理函数的形式. 同样地，利用 (3.5)~(3.7) 式，也可以用 X, Y 表示出 g_2, h_2. 将这些结果代入 $Dg_2 - 2(h_2 + a_1 g_2 + a_3)$ 和 $Dh_2 - 2(3g_2^2 + 2a_2 g_2 + a_4 - a_1 h_2)$，化简并约去 Y 的最高项，即可得

$$\begin{aligned}
Dg_2 &= 2(2h_2 + a_1 g_2 + a_3), \\
Dh_2 &= 2(3g_2^2 + 2a_2 g_2 + a_4 - a_1 h_2).
\end{aligned}$$

当 $m>2$ 时，利用点加公式 (参见推论 3.10) 可得

$$\lambda = \frac{h_{m-1}-Y}{g_{m-1}-X}, \tag{3.11}$$

$$g_m = -g_{m-1}-X+\lambda^2+a_1\lambda-a_2, \tag{3.12}$$

$$h_m = -(\lambda+a_1)g_m-a_3-Y+\lambda X, \tag{3.13}$$

$$D\lambda = \frac{(Dh_{m-1}-DY)(g_{m-1}-X)}{(g_{m-1}-X)^2} - \frac{(h_{m-1}-Y)(Dg_{m-1}-DX)}{(g_{m-1}-X)^2}, \tag{3.14}$$

$$Dg_m = -Dg_{m-1}-DX+2\lambda D\lambda+a_1D\lambda, \tag{3.15}$$

$$Dh_m = -(\lambda+a_1)Dg_m-g_mD\lambda-DY+\lambda DX+XD\lambda. \tag{3.16}$$

由归纳假设可得

$$Dg_{m-1} = (m-1)(2h_{m-1}+a_1g_{m-1}+a_3), \tag{3.17}$$

$$Dh_{m-1} = (m-1)(3g_{m-1}^2+2a_2g_{m-1}+a_4-a_1h_{m-1}). \tag{3.18}$$

由此利用 (3.4) 以及以上的等式就可以将 $Dg_m-m(2h_m+a_1g_m+a_3)$, $Dh_m-m(3g_m^2+2a_2g_m+a_4-a_1h_m)$ 用 X, Y, g_{m-1}, h_{m-1} 表示. 注意到 (X,Y), (g_{m-1},h_{m-1}) 都是有理映射，因此就可以约去 Y^2, h_{m-1}^2，从而即可证定理成立. □

对于多项式 $f\in K[X]$，众所周知 $f'=0$ 的充要条件是 $f=f_1(X^p)$，其中 f_1 是某个多项式. 对于有理函数有一个类似的结论.

引理3.28　设 $v\in K(X)$ 是一个单变量的有理函数，则

$$v'=0 \Longleftrightarrow v=v_1(X^p),$$

其中 $v_1\in K(X)$.

证明　显然当特征为 p 时，

$$\frac{\partial v_1(X^p)}{\partial X} = pX^{p-1}v_1'(X^p)=0.$$

反之，设 $v=\dfrac{f}{g}$，其中 f, g 是 $K[X]$ 中互素的多项式，则由

$$0=v'=\frac{f'g-fg'}{g^2}$$

知

$$f'g = fg',$$

因此 $f|f'$, $g|g'$. 由于 $\deg f' < \deg f$(若 $f=0$, 则引理显然成立), $\deg g' < \deg g$, 可得 $f'=g'=0$. 由此可知对适当的多项式 f_1, $g_1 \in K[X]$, 有 $f = f_1(X^p)$, $g = g_1(X^p)$, 从而 $v = \dfrac{f_1}{g_1}(X^p)$. □

定理3.29 设 $r \in K(E)$, $p > 0$, 则

$$Dr = 0 \Longleftrightarrow r = r_1(X^p, Y^p),$$

其中 $r_1 \in K(E)$.

证明 如果 $Dr = 0$, 则由命题 3.25 知 $Dr_1(X^p, Y^p) = 0$. 反之我们首先说明 $Y^p \notin K(X)$: 若 $p=2$, 则有

$$Y^2 = (a_1X + a_3)Y + (X^3 + a_2X^2 + a_4X + a_6)$$

且 $a_1X + a_3 \neq 0$, 因此由 $Y \notin K(X)$ 可得 $Y^2 \notin K(X)$. 若 $p \neq 2$, 则 Y^p 是多项式.

$$T^2 + a_1^pX^pT + a_3^pT - (X^{3p} + a_2^pX^{2p} + a_4^pX^p + a_6^p) \in K(X)[T]$$

的根. 利用 2.2 节中证明 Weierstrass 方程不可约的证明方法, 同样可以证明上面的多项式是 $K(X)$ 中的不可约多项式. (原方法的关键是 $\deg f + \deg g = 3$ 是奇数, 而这里 $\deg f + \deg g = 3p$ 也是奇数.)

由此可知 $K(X) \subsetneqq K(X, Y^p) \subseteq K(E)$, 从而由

$$2 = [K(E):K(X)] = [K(E):K(X,Y^p)][K(X,Y^p):K(X)]$$

知 $K(X, Y^p) = K(E)$ 且 $\{1, Y^p\}$ 是 $K(E)$ 在 $K(X)$ 上的一组基. 因此 $r \in K(E)$ 可表示为 $r = u + Y^pv$ 的形式, 其中 u, $v \in K(X)$. 更进一步地, 记 $Y^p = f + gY$, f, $g \in K(X)$, $g \neq 0$. 又记 $t = a_1X + a_3$, $s = X^3 + a_2X^2 + a_4X + a_6$, 则

$$Dr = (u' + Y^pv')DX + pY^{p-1}vDY = (u' + Y^pv')DX.$$

由于 $Dr = 0$, $DX \neq 0$, 因此 $u' + Y^pv' = 0$. 由于 $\{1, Y^p\}$ 是一组基, 因此有 $u' = v' = 0$. 利用引理 3.28 知 $u = u_1(X^p)$, $v = v_1(X^p)$, 所以 $r = r_1(X^p, Y^p)$, 其中 $r_1 = u_1 + Yv_1$. □

下面我们试图寻找有理函数及其导数在零点和极点的阶数之间的关系. 对于在特征为 0 的域上的多项式 f, 我们已经知道: 如果 f 在 x 处有 $d>0$ 阶零点, 则 f' 在 x 处有 $d-1$ 阶零点. 对于一般有理函数, 在考虑域特征的情况下, 也有类似的结论.

定理3.30　*设 r 是一个有理函数, $P\in E$, $d=\mathrm{ord}_P(r)$, 则*

- *若 $p\nmid d$, 则 $\mathrm{ord}_P(Dr)=d-1$.*
- *若 $p\mid d$, 则 $\mathrm{ord}_P(Dr)\geqslant d$.*

证明　我们约定, 当 $p=0$ 时, 如果 $d>0$, 就应用第一个结论, 如果 $d=0$, 就应用第二个结论. 首先我们考虑 $d=0$. 若 $P\neq\mathcal{O}$, 记 $r=\dfrac{f}{g}$, $f(P)$, $g(P)\neq 0$, 则 $Dr=\dfrac{gDf-fDg}{g^2}$ 在 P 点处是正则的. 若 $P=\mathcal{O}$, 记 $r=u+vY$, u, $v\in K(X)$, 则由引理 2.31 可得

$$0=d=\mathrm{ord}_{\mathcal{O}}r=\min\{-2\deg u,\quad -3-2\deg v\},$$

因此 $\deg u=0$[①]. 由此可知如果 $u=\dfrac{f_1}{g_1}$, f_1, $g_1\in K[X]$, 则多项式 f_1, g_1 次数相等. 不妨设 f_1, g_1 的次数均为 n. 对于 $Du=\dfrac{f_1'g_1-f_1g_1'}{g_1^2}DX$, 考虑 $f_1'g_1-f_1g_1'$ 的次数:

1. 当 $p\nmid n$ 时, $\deg(f_1'g_1)=\deg(f_1g_1')=2n-1$ 且两者的首项系数相等;
2. 当 $p\mid n$ 时, $\deg(f_1'g_1)$, $\deg(f_1g_1')\leqslant 2n-2$,

所以 $\deg(f_1'g_1-f_1g_1')\leqslant 2n-2$, 因此

$$\mathrm{ord}_{\mathcal{O}}\left(\frac{f_1'g_1-f_1g_1'}{g_1^2}\right)\geqslant 4.$$

又由于 $\mathrm{ord}_{\mathcal{O}}DX\geqslant -3$, 所以有 $\mathrm{ord}_{\mathcal{O}}(Du)\geqslant 1$. 同时又由 $-3-2\deg v\geqslant 0$, 知 $-2\deg v\geqslant 4$. 由 $\deg v'\leqslant \deg v-1$ 可知 $-2\deg v'\geqslant -2\deg v+2\geqslant 6$. 再由引理 2.31 可知

$$\mathrm{ord}_{\mathcal{O}}(2Y+a_1X+a_3)\geqslant -3,\quad \mathrm{ord}_{\mathcal{O}}(3X^2+2a_2X+a_4-a_1Y)\geqslant -4,$$

因此

① 由于 $\deg v$ 是整数, 因此 $-3-2\deg v<0$, 所以 $\deg u=0$ —— 译者注.

$$\begin{aligned}\mathrm{ord}_{\mathcal{O}}(v'YDX+vDY) \geqslant& \min\{6-3+\mathrm{ord}_{\mathcal{O}}(2Y+a_1X+a_3),\\ & 4+\mathrm{ord}_{\mathcal{O}}(3X^2+2a_2X+a_4-a_1Y)\}\\ \geqslant& 0.\end{aligned}$$

利用

$$\begin{aligned}Dr &= Du+v'YDX+vDY\\ &= Du+v'Y(2Y+a_1X+a_3)+v(3X^2+2a_2X+a_4-a_1Y).\end{aligned}$$

即可得

$$\mathrm{ord}_{\mathcal{O}}(Dr) \geqslant \min\{\mathrm{ord}_{\mathcal{O}}Du,\quad \mathrm{ord}_{\mathcal{O}}(v'YDX+vDY)\} \geqslant 0.$$

当 $d=1$ 时，设 u 是 P 点处的一致化参数，则 $r=u\varepsilon$，其中 $\mathrm{ord}_P\varepsilon=0$，因此

$$\mathrm{ord}_P(Dr)=\mathrm{ord}_P(\varepsilon Du+uD\varepsilon).$$

如果能够证明 $\mathrm{ord}_P(Du)=0$，则由 $\mathrm{ord}_P(\varepsilon Du)=\mathrm{ord}_P\varepsilon+\mathrm{ord}_P(Du)=0$，以及 $d=0$ 时得到的 $\mathrm{ord}_P(uD\varepsilon)=1+\mathrm{ord}_P(D\varepsilon)\geqslant 1$ 就可以得到 $\mathrm{ord}_P(Dr)=0$. 下面分情况证明 $\mathrm{ord}_P(Du)=0$：

- 当 $P=(x,y)\notin E[2]$，即 $2y+a_1x+a_3\neq 0$，$u=X-x$ 时，有 $Du=DX=2Y+a_1X+a_3$ 在 P 点处正则且不等于零.
- 当 P 是一个 2 阶点且 $p\neq 2$ 时，此时有 $u=2Y+a_1X+a_3=\dfrac{\partial E}{\partial Y}$. 由此利用 E 的非奇异性可知
$$\frac{\partial E}{\partial Y}(P)=0,\quad \frac{\partial E}{\partial X}(P)\neq 0,$$
因此
$$Du(P)=2DY(P)+a_1DX(P)=2\frac{\partial E}{\partial X}(P)+a_1\frac{\partial E}{\partial Y}(P)\neq 0.$$
- 当 P 是 2 阶点且 $p=2$ 时，取 $u=Y+y$，则与前一种情况相同地可得
$$\frac{\partial E}{\partial Y}(P)=0,\quad \frac{\partial E}{\partial X}(P)\neq 0,$$
因此
$$Du(P)=DY=\frac{\partial E}{\partial X}(P)\neq 0.$$
- 当 $P=\mathcal{O}$ 时，取 $u=\dfrac{X}{Y}$

$$
\begin{aligned}
Du &= \frac{YDX - XDY}{Y^2} \\
&= \frac{Y(2Y + a_1X + a_3) - X(3X^2 + 2a_2X + a_4 - a_1Y)}{Y^2} \\
&= \frac{-X^3 + a_4X + 2a_6 - a_3Y}{X^3 + a_2X^2 + a_4X + a_6 - (a_1X + a_3)Y}, \\
\mathrm{ord}_{\mathcal{O}}(Du) &= -6 - (-6) = 0. \quad (\text{引理 } 2.31)
\end{aligned}
$$

最后当 $d \geqslant 2$ 时，记 $r = u^d r_1$，其中 u 是 P 点处的一致化参数，$\mathrm{ord}_P r_1 = 0$，则

$$
\begin{aligned}
Dr &= du^{d-1} r_1 Du + u^d Dr_1 \\
&= u^{d-1}(dr_1 Du + uDr_1),
\end{aligned}
$$

其中 $\mathrm{ord}_P(uDr_1) \geqslant 1$ 且 $\mathrm{ord}_P(r_1Du) = 0$. 若 $p \nmid d$，则有 $\mathrm{ord}_P(Dr) = d-1$；若 $p \mid d$，则 $Dr = u^d Dr_1$，因此 $\mathrm{ord}_P(Dr) \geqslant d$. □

最后用下面的命题结束本节. 该命题表明导数运算与 m 乘映射是几乎 "可交换的".

命题3.31 设 m 是一个整数，r 是一个有理函数，则

$$D(r \circ [m]) = mDr \circ [m].$$

证明 容易看到满足命题要求的有理函数在域运算下是封闭的，因此只需分别考虑 $r = X$，$r = Y$ 的情况即可. 如果 $m > 0$，则就是定理 3.27. 若 $m = 0$，则命题显然成立. 当 $m = -1$ 时，有

$$
\begin{aligned}
D(X \circ [-1]) &= DX \\
&= 2Y + a_1X + a_3 \\
&= -(2(-Y - a_1X - a_3) + a_1X + a_3) \\
&= -DX \circ [-1], \\
D(Y \circ [-1]) &= D(-Y - a_1X - a_3) \\
&= -((3X^2 + 2a_2X + a_4) - a_1(-Y - a_1X - a_3)) \\
&= -DY \circ [-1].
\end{aligned}
$$

当 $m < -1$ 时，由已经证明的结论可得

$$
\begin{aligned}
D(r \circ [m]) &= D(r \circ [-m] \circ [-1]) \\
&= -D(r \circ [-m]) \circ [-1] \\
&= -(-m)Dr \circ [-m] \circ [-1] \\
&= mDr \circ [m].
\end{aligned}
$$

□

3.4 可 分 性

在本节中我们将确定 $e_{[m]}$ 以及一类非常重要的自同态的分歧指数 .

要注意在本节中我们假设域特征 $p>0$.

定义3.32 *如果对于非零自同态 α, 有 $e_\alpha=1$, 则称其是可分的, 否则称其是不可分的.*

实际上, "可分" 的定义与 3.2 节中 "非分歧" 的定义是一致的. 这是由于如果 α 是可分自同态, 则扩域 $K(E)/\alpha^*(K(E))$ 是可分扩张.

命题3.33 *对于非零自同态 α, 以下的论断是等价的:*

1. *α 是不可分的;*
2. *$D(r\circ\alpha)=0,\quad \forall r\in K(E)$;*
3. *存在有理函数 r, s, 满足 $\alpha=(r(X^p,Y^p),\ s(X^p,Y^p))$.*

证明

1. $\Rightarrow$ 2.

假设 α 是不可分的, r 是有理函数并且 $D(r\circ\alpha)\neq 0$, 则 $D(r\circ\alpha)$ 只有有限多个零点和极点, 因此必存在点 $P\in E$, 使得 $D(r\circ\alpha)$ 在 P 点有定义并且不等于零. 记 $s:=r-(r\circ\alpha)(P)$, 则 $s\circ\alpha(P)=0$, 即有 $\mathrm{ord}_P(s\circ\alpha)\geqslant 1$. 另一方面, 由于 $D(s\circ\alpha)(P)=D(r\circ\alpha)(P)\neq 0$, 因此 $\mathrm{ord}_P(D(s\circ\alpha))=0$, 由定理 3.30 知 $\mathrm{ord}_P(s\circ\alpha)=1$. 但由 $e_\alpha>1$ 及引理 3.14 知 $\mathrm{ord}_P(s\circ\alpha)=e_\alpha\mathrm{ord}_{\alpha(P)}(s)>1$, 矛盾.

2. $\Rightarrow$ 3.

分别令 $r=X$ 及 $r=Y$, 则由定理 3.29 即可得证该论断.

3. $\Rightarrow$ 1.

由 e_α 的定义以及 $\dfrac{X}{Y}$ 是 $\mathcal{O}$ 处的一致化参数 (参见定理 2.26) 可得

$$e_\alpha=\mathrm{ord}_{\mathcal{O}}\left(\frac{X}{Y}\circ\alpha\right)=\mathrm{ord}_{\mathcal{O}}\left(\frac{r(X^p,Y^p)}{s(X^p,Y^p)}\right).$$

计算 $D\left(\dfrac{X}{Y}\circ\alpha\right)$ 如下:

$$D\left(\frac{X}{Y}\circ\alpha\right)=\frac{s(X^p,Y^p)D(r(X^p,Y^p))-r(X^p,Y^p)D(s(X^p,Y^p))}{s(X^p,Y^p)^2},$$

由于

$$D(r(X^p, Y^p)) = \frac{\partial(r(X^p, Y^p))}{\partial X}DX + \frac{\partial(r(X^p, Y^p))}{\partial Y}DY \quad (\text{命题 } 3.24)$$
$$= 0.$$

同样地可以证明 $D(s(X^p, Y^p)) = 0$, 因此

$$D\left(\frac{X}{Y}\circ\alpha\right) = 0, \quad \mathrm{ord}_{\mathcal{O}}\left(D\left(\frac{X}{Y}\circ\alpha\right)\right) \geqslant 1.$$

由定理 3.30, 可知

$$\mathrm{ord}_{\mathcal{O}}\left(\frac{X}{Y}\circ\alpha\right) > 1.$$

因此 α 是不可分的. □

推论3.34　设 α, β 是两个非零自同态, 则

1. 如果 α, β 是不可分的, 则 $\alpha + \beta$ 也是不可分的.
2. 如果 α 是可分的, β 是不可分的, 则 $\alpha + \beta$ 必定是可分的.

证明

1. 该结论由命题 3.33 中的第三条显然可得.
2. 如果 $\alpha + \beta$ 是不可分的, 则由第一条知 $\alpha = (\alpha + \beta) - \beta$ 也是不可分的, 矛盾.

□

命题3.35　如果 m 与 p 互素, 则 $[m]$ 是可分的.

证明　设 $P \in E$, u 是 mP 点处的一致化参数, 则 $e_{[m]} = \mathrm{ord}_P(u \circ [m])$. 由命题 3.31 知

$$D(u \circ [m]) = mDu \circ [m].$$

由此可知

$$\mathrm{ord}_P(D(u \circ [m])) = \mathrm{ord}_P(Du \circ [m])$$
$$= e_{[m]}\mathrm{ord}_{mP}(Du) \quad (\text{引理 } 3.14)$$
$$= 0 \quad (\text{定理 } 3.30).$$

再次利用定理 3.30 可得 $\mathrm{ord}_P(u \circ [m]) = 1$. □

推论3.36　如果 $k = \mathbb{F}_q$, m, n 是整数且 m, p 互素, 则 $[m] + [n] \circ \varphi$ 是可分的.

证明 由推论 3.18 以及命题 3.19 可知

$$e_{[n]\circ\varphi} = e_{[n]}e_{\varphi} = qe_{[n]} > 1,$$

因此 $[n]\circ\varphi$ 是不可分的. 由于 $[m]$ 是可分的，因此由推论 3.34 知结论成立. □

3.5 m 扭 点

本节主要将讨论 $E[m]$ 的群结构. 具体而言就是要证明以下的结论：

命题3.37 如果 $\gcd(m,p)=1$，则

$$E[m] \simeq \mathbb{Z}_m \times \mathbb{Z}_m.$$

命题3.38 若 $E[p] \neq \{\mathcal{O}\}$，则

$$E[p^v] \simeq \mathbb{Z}_{p^v}.$$

利用群的基本理论，可以将以上的两个结论归结为下面的定理：

定理3.39 设 m 是一个正整数，$m = p^v m'$ 其中 $p \nmid m'$.

- 如果 $E[p] = \{\mathcal{O}\}$，则

$$E[m] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m'}.$$

- 否则

$$E[m] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_m.$$

在此我们通过考察 g_m，h_m 以及 $g_m - g_n$ 的除子来证明该定理. 由于我们采用的方法不需要非常多的理论知识，但这样就需要比较大量的计算，且需单独考虑特征等于 2, 3 时的情况. 虽然用手工的方式也可以完成所需的计算，但利用符号代数软件无疑会提供非常大的帮助. 为表述更加简洁，我们首先介绍下面的概念：

定义3.40 设 r 是一个有理函数，则称

$$l(r) := \left(\left(\frac{X}{Y}\right)^{-\mathrm{ord}_{\mathcal{O}} r} r\right)(\mathcal{O})$$

是 r 在 $\mathcal{O}$ 处的首项系数.

l 是 $K(E)^{\times}$ 到 $K^{\times}$ 上的 (乘法) 同态. 同时由命题 2.14 知：若有理函数 r, s 满足 $\mathrm{ord}_{\mathcal{O}}r = \mathrm{ord}_{\mathcal{O}}s$, 则 $\mathrm{ord}_{\mathcal{O}}(r+s) = \mathrm{ord}_{\mathcal{O}}r = \mathrm{ord}_{\mathcal{O}}s$ 的充要条件是 r, s 首项系数之和不等于零. 此时有 $l(r+s) = l(r) + l(s)$. 由于 X, Y 的首项系数等于 1, 因此将 X, Y 的幂次乘以某个有理函数并不会改变该有理函数的首项系数.

在此我们需要了解 g_m 在 $\mathcal{O}$ 处的阶及其首项系数. 和以往一样, 我们仍然对 m 进行归纳. 但需要进行一些调整, 因为得到的大多数结论都要求 m, p 互素. 首先考察 g_p, $p \in \{2, 3\}$, 得到的第一个结论如下：

命题3.41　设 $p \in \{2, 3\}$, 则

$$|E[p]| = \begin{cases} p, & j \neq 0, \\ 1, & j = 0. \end{cases}$$

证明　由 2.5 节知, 当 $p = 2$ 时命题是显然成立的..当 $p = 3$ 时, 由于 E 上的有限点 $P \in E[3]$ 的充要条件是 $2P = \pm P$, 即 $X(2P) = X(P)$, 也就是 $(g_2 - X)(P) = 0$. 由计算可得

$$g_2 - X = \frac{-b_2X^3 - b_8}{(-Y + a_1X + a_3)^2},$$

其中 b_2, b_8 参见定义 2.7. 由于特征 $p = 3$, 因此当 $b_2 \neq 0$, 即 $j = \dfrac{b_2^6}{\Delta} \neq 0$ 时, 分子有唯一的根 $x = \sqrt[3]{-\dfrac{b_8}{b_2}}$, 其对应着 E 上的点 $P = (x, y)$ 和 $Q = \overline{P}$, 其中 y 是 $E(x, Y)$ 的根. 由引理 2.31 知分子在 $\mathcal{O}$ 处有 6 阶极点, 因此其除子必定为 $3\langle P\rangle + 3\langle Q\rangle - 6\langle\mathcal{O}\rangle$. 而分母的除子为 $2\langle R_1\rangle + 2\langle R_2\rangle + 2\langle R_3\rangle - 6\langle\mathcal{O}\rangle$, 其中 R_i 是三个不同的 2 阶点. 由此可知 $\mathrm{ord}_P(g_2 - X)$, $\mathrm{ord}_Q(g_2 - X) \geqslant 1$, 则 $E[3] = \{P, Q, \mathcal{O}\}$. 另一方面, 如果 $b_2 = 0$, 即 $j = 0$, 此时 $g_2 - X$ 没有零点, 从而有 $E[3] = \{\mathcal{O}\}$. □

命题3.42　设 $p \in \{2, 3\}$, 定义

$$\alpha = \frac{p^2}{|E[p]|} = \begin{cases} p, & j \neq 0, \\ p^2, & j = 0, \end{cases}$$

则

$$\mathrm{ord}_{\mathcal{O}}g_p = -2\alpha, \quad \mathrm{ord}_{\mathcal{O}}h_p = -3\alpha.$$

首项系数分别是

$$l(g_p) = \frac{1}{\gamma^2}, \quad l(h_p) = \frac{1}{\gamma^3},$$

其中

$$\gamma = \begin{cases} a_1, & p=2 \text{ 且 } j \neq 0, \\ a_3, & p=2 \text{ 且 } j=0, \\ a_1^2+a_2, & p=3 \text{ 且 } j\neq 0, \\ (a_1a_3-a_4)^2, & p=3 \text{ 且 } j=0. \end{cases}$$

证明

- 设 $p=2$，我们分别对 $j\neq 0$ 和 $j=0$ 两种情况进行考察. 要注意我们并不要求曲线是标准形式的.

  —— 当 $j\neq 0$，即 $a_1\neq 0$ 时，由倍点计算公式可知

$$\lambda = \frac{X^2+a_4+a_1Y}{a_1X+a_3},$$
$$g_2 = \lambda^2+a_1\lambda+a_2,$$
$$h_2 = \lambda(g_2+X)+Y+(a_1g_2+a_3).$$

  由引理 2.31 知 λ 在 $\mathcal{O}$ 处有 2 阶极点且 $l(\lambda)=\dfrac{1}{a_1}$，所以 g_2 在 $\mathcal{O}$ 处有 4 阶极点且 $l(g_2)=l(\lambda^2)=\dfrac{1}{a_1^2}$，而 h_2 在 $\mathcal{O}$ 处有 6 阶极点且 $l(h_2)=l(\lambda)l(g_2)=\dfrac{1}{a_1^3}$.

  —— 当 $j=0$，即 $a_1=0$ 时，由倍点计算公式可知

$$\lambda = \frac{X^2+a_4}{a_3},$$
$$g_2 = \lambda^2+a_2,$$
$$h_2 = \lambda(g_2+X)+Y+a_3.$$

  用和前面相同的方法同样可证命题成立.

- 设 $p=3$，由定义 2.7 可知

$$c_4=b_2^2=(a_1^2+a_2)^2, \quad b_4=a_1a_3-a_4, \quad j=\frac{(a_1^2+a_2)^6}{\Delta}.$$

所以 $j=0$ 也就意味着 $b_2=a_1^2+a_2=0$. 首先利用倍点公式计算 g_2，h_2 如下：

$$\lambda_2 = \frac{-a_2X+a_4-a_1Y}{-Y+a_1X+a_3},$$
$$g_2 = X+\lambda_2^2+a_1\lambda_2-a_2,$$

$$h_2 = -\lambda_2(g_2 - X) - Y - (a_1 g_2 + a_3).$$

由引理 2.31 知 $\mathrm{ord}_{\mathcal{O}}\lambda_2 \geqslant 0$, 因此

$$\mathrm{ord}_{\mathcal{O}} g_2 = \mathrm{ord}_{\mathcal{O}} X = -2, \quad l(g_2) = l(X) = 1,$$

$$\mathrm{ord}_{\mathcal{O}} h_2 = \mathrm{ord}_{\mathcal{O}}(-Y) = -3, \quad l(h_2) = -l(Y) = -1.$$

再计算 g_3, h_3 如下:

$$\begin{aligned} \lambda &= \frac{h_2 - Y}{g_2 - X}, \\ g_3 &= \lambda^2 + (-g_2 - X + a_1\lambda - a_2), \\ h_3 &= -\lambda g_3 + (\lambda X - Y - a_1 g_3 - a_3), \end{aligned}$$

将 h_2, g_2 代入 λ 并约去 Y 的高次项可得

$$\lambda = \frac{(X^6 + \cdots) + a_1 b_2 (X^3 + \cdots)t}{(b_2 X^3 + \cdots)t},$$

其中 $t = -Y + a_1 X + a_3$ 在 $\mathcal{O}$ 处有 3 阶极点且首项系数为 -1, 而省略号表示次数较低的项, 因此当 $j \neq 0$ 时, $\mathrm{ord}_{\mathcal{O}}\lambda = -3$, $l(\lambda) = -\dfrac{1}{b_2}$. 当 $j = 0$ 时, 有

$$\lambda = \frac{X^6 + \cdots}{b_4^2 t},$$

因此 λ 在 $\mathcal{O}$ 处的阶为 -9, 而首项系数为 $-\dfrac{1}{b_4^2}$. 注意到无论哪种情况, g_3 中阶最低的项都是 λ^2, 因此

$$\mathrm{ord}_{\mathcal{O}} g_3 = 2\mathrm{ord}_{\mathcal{O}}\lambda, \quad l(g_3) = l(\lambda)^2,$$

而 h_3 中阶最低的项是 $-\lambda g_3$, 因此有

$$\mathrm{ord}_{\mathcal{O}} h_3 = 3\mathrm{ord}_{\mathcal{O}}\lambda, \quad l(h_3) = -l(\lambda)^3. \qquad \square$$

下面得到的结论对任意特征都是成立的.

命题3.43 设 m 是与 p 互素的正整数, 则 g_m, h_m 在 $\mathcal{O}$ 处分别有 2 阶和 3 阶极点, 其首项系数分别为 $l(g_m) = \dfrac{1}{m^2}, l(h_m) = \dfrac{1}{m^3}$.

证明 我们对 m 进行归纳. 但要注意的是当在归纳过程中遇到 p 的倍数时, 归纳过程就会中断, 因为此时并不满足命题的前提条件. 为此我们的对策是从 $m-1$ 直接过渡到 $m+1$. 下面的证明需要区分很多种情况, 为了保证总体想法的完整性, 首先假设 $p \notin \{2,3\}$. 要注意的是这里我们所说的 "首项系数之和不等于零" 是对 $\mathbb{F}_p$, 而不是对 $\mathbb{Q}$ 而言的 (当然除了 $p=0$ 的情况).

1. 当 $m=1$ 时, 有 $g_1 = X$, $h_1 = Y$, 因此由引理 2.31 知命题成立.
2. 当 $m=2$ 时, 由倍点计算公式可得

$$\begin{aligned}\lambda &= \frac{3X^2 + 2a_2X + a_4 - a_1Y}{2Y + a_1X + a_3},\\ g_2 &= -2X + \lambda^2 + (a_1\lambda - a_2),\\ h_2 &= -\lambda(g_2 - X) - Y - (a_1g_2 + a_3).\end{aligned}$$

由引理 2.31 知, λ 在 $\mathcal{O}$ 处有一阶极点, 因此

$$\mathrm{ord}_{\mathcal{O}}(-2X) = -2, \quad \mathrm{ord}_{\mathcal{O}}(\lambda^2) = -2, \quad \mathrm{ord}_{\mathcal{O}}(a_1\lambda - a_2) \geqslant -1.$$

如果能够说明 $-2X + \lambda^2$ 的首项系数等于 $\frac{1}{4}$, 那么对于 g_2 就完成了命题的证明:

$$\begin{aligned}l(\lambda) &= \frac{\lambda X}{Y}(\mathcal{O})\\ &= \frac{(3X^2 + 2a_2XZ + a_4Z^2 - a_1YZ)X}{(2YZ + a_1XZ + a_3Z^2)Y}(0,1,0)\\ &= \frac{(3X^2 + 2a_2XZ + a_4Z^2 - a_1Z)X}{(2Z + a_1XZ + a_3Z^2)}(0,0)\\ &= \frac{3}{2}.\end{aligned}$$

(由定理 2.26 的证明可知在 E_* 上 X 是一致化参数, 而 Z 在 $(0,0)$ 处的阶等于 3.)

$$l(g_2) = -2 + l(\lambda)^2 = \frac{1}{4}.$$

对于 h_2, 由于 g_2, X 在 $\mathcal{O}$ 处都有 2 阶极点且其首项系数并不相互抵消, 因此 $\mathrm{ord}_{\mathcal{O}}(g_2 - X) = -2$, 所以 $\mathrm{ord}_{\mathcal{O}}(-\lambda(g_2 - X)) = -3$. 同时 $\mathrm{ord}_{\mathcal{O}}(-Y) = -3$, $\mathrm{ord}_{\mathcal{O}}(a_1g_2 + a_3) \geqslant -2$. 和对 g_2 的做法类似, 我们下面说明 $-\lambda(g_2 - X)$, $-Y$ 的首项系数之和等于 $\frac{1}{8}$:

$$l(-\lambda(g_2 - X)) = -l(\lambda)(l(g_2) - l(X)) = -\frac{3}{2}\left(\frac{1}{4} - 1\right) = \frac{9}{8},$$

$$l(h_2) = \frac{9}{8} - 1 = \frac{1}{8}.$$

3. 假设对于 $m-1$ 命题成立，其中 $m \not\equiv 0, 1, 2 \pmod p$，下面说明命题对 m 也成立. 此时由加法公式可得

$$\begin{aligned}
\lambda &= \frac{h_{m-1} - Y}{g_{m-1} - X}, \\
g_m &= -g_{m-1} - X + \lambda^2 + (a_1\lambda - a_2), \\
h_m &= -\lambda(g_m - X) - Y - (a_1 g_m + a_3).
\end{aligned}$$

要注意 $\mathrm{ord}_{\mathcal{O}}(g_{m-1} - X) = -2$. 这是由于其首项系数并不为零：

$$\begin{aligned}
& l(g_{m-1}) - l(X) = 0 \\
\Longleftrightarrow & \frac{1}{(m-1)^2} - 1 \equiv 0 \pmod p \quad (\text{归纳假设}) \\
\Longleftrightarrow & (m-1)^2 \equiv 1 \pmod p \\
\Longleftrightarrow & m - 1 \equiv \pm 1 \pmod p \\
\Longleftrightarrow & m = 0 \text{ 或 } 2. \pmod p
\end{aligned}$$

下面再分两种情况加以讨论：

- 当 $(m-1)^3 \not\equiv 1 \pmod p$ 时，与 g_{m-1}，X 类似地可以证明 h_{m-1}，Y 的首项系数是不相同的，因此由归纳假设可知 $\mathrm{ord}_{\mathcal{O}}\lambda = -1$，且

$$l(\lambda) = \frac{l(h_{m-1}) - l(Y)}{l(g_{m-1}) - l(X)} = \frac{\dfrac{1}{(m-1)^3} - 1}{\dfrac{1}{(m-1)^2} - 1} = \frac{m^2 - m + 1}{m(m-1)}.$$

  在 g_m 中，$\mathrm{ord}_{\mathcal{O}}(a_1\lambda - a_2) \geqslant -1$，而其他的项在 $\mathcal{O}$ 处的阶都等于 -2 且它们的首项系数之和不等于零：

$$\begin{aligned}
l(g_m) &= -l(g_{m-1}) - l(X) + l(\lambda)^2 \\
&= -\frac{1}{(m-1)^2} - 1 + \left(\frac{m^2 - m + 1}{m(m-1)}\right)^2 \\
&= \frac{1}{m^2}.
\end{aligned}$$

  对于 h_m 同样地有：

$$\begin{aligned} l(h_m) &= -l(\lambda)(l(g_m) - l(X)) - l(Y) \\ &= -\frac{m^2 - m + 1}{m(m-1)} \cdot \frac{1 - m^2}{m^2} - 1 \\ &= \frac{1}{m^3}. \end{aligned}$$

- 当 $(m-1)^3 \equiv 1 \pmod p$ 时，有 $l(h_{m-1}) = l(Y) = 1$，因此 $\text{ord}_{\mathcal{O}}(h_{m-1} - Y) \geqslant -2$，从而 λ 在 $\mathcal{O}$ 处是正则的. 在 g_m 的表示式中，除 $-g_{m-1} - X$ 以外，其余各项在 $\mathcal{O}$ 都是正则的. 注意到 $\text{ord}_{\mathcal{O}}(-g_{m-1} - X) = -2$ 而首项系数为

$$-\frac{1}{(m-1)^2} - 1 = -\frac{(m-1) + (m-1)^3}{(m-1)^3} = -m = \frac{-m^3}{m^2}.$$

而由 $(m-1)^3 \equiv 1 \pmod p$ 可知

$$\begin{aligned} 0 &= (m-1)^3 - 1 \\ &= m^3 - 3m^2 + 3m - 2 \\ &= (m^3 + 1)\left(1 - \frac{3}{m+1}\right). \end{aligned}$$

因为 $m + 1 \not\equiv 3 \pmod p$，所以在 $\mathbb{F}_p$ 中有 $-m^3 = 1$，因此 $l(g_m) = \dfrac{1}{m^2}$. 对于 h_m，其首项系数为

$$l(h_m) = -l(Y) = -1 = \frac{1}{m^3}.$$

4. 假设对于 $m-2$ 命题成立，其中 $m \equiv 1 \pmod p$. 现在证明对于 m 命题也成立. 由于 $p \neq 3$，因此有 $m \neq 4$，从而由推论 3.10 可知 $[m-2] \neq [2]$. 由此对 $[m-2]$, $[2]$ 利用加法公式可得

$$\begin{aligned} \lambda &= \frac{h_{m-2} - h_2}{g_{m-2} - g_2}, \\ g_m &= -g_{m-2} - g_2 + \lambda^2 + (a_1\lambda - a_2), \\ h_m &= -\lambda(g_m - g_2) - h_2 - (a_1 g_m + a_3). \end{aligned}$$

和前面类似地可得 $\text{ord}_{\mathcal{O}}\lambda = -1$，且

$$\begin{aligned} l(\lambda) &= \frac{l(h_{m-2}) - l(h_2)}{l(g_{m-2}) - l(g_2)} = \frac{\dfrac{1}{(m-2)^3} - \dfrac{1}{8}}{\dfrac{1}{(m-2)^2} - \dfrac{1}{4}} \\ &= \frac{\dfrac{1}{(-1)^3} - \dfrac{1}{8}}{\dfrac{1}{(-1)^2} - \dfrac{1}{4}} = -\frac{3}{2} \neq 0, \quad \infty, \end{aligned}$$

$$
\begin{aligned}
l(g_m) &= -l(g_{m-2}) - l(g_2) + l(\lambda)^2 \\
&= -\frac{1}{(-1)^2} - \frac{1}{4} + \frac{9}{4} \\
&= 1 \\
&= \frac{1}{m^2}, \\
l(h_m) &= -l(\lambda)(l(g_m) - l(g_2)) - l(h_2) \\
&= \frac{3}{2}\left(1 - \frac{1}{4}\right) - \frac{1}{8} \\
&= 1 \\
&= \frac{1}{m^3}.
\end{aligned}
$$

5. 假设对于 $m-3$ 命题成立，其中 $m \equiv 2 \pmod p$. 现在证明对于 m 命题也成立. 由于 $p \neq 2, 3$, 因此 $m \neq 6$. 由于在第三种情况中，我们已经证明了命题对 [3] 是成立的，因此对 $[m-3]$, [3] 利用加法公式可得

$$
\begin{aligned}
\lambda &= \frac{h_{m-3} - h_3}{g_{m-3} - g_3}, \\
g_m &= -g_{m-3} - g_3 + \lambda^2 + (a_1\lambda - a_2), \\
h_m &= -\lambda(g_m - g_3) - h_3 - (a_1 g_m + a_3).
\end{aligned}
$$

由于 $g_{m-3} - g_3$ 的首项系数为

$$
\frac{1}{(m-3)^2} - \frac{1}{9} = 1 - \frac{1}{9} = \frac{8}{9} \neq 0,
$$

因此 $\mathrm{ord}_{\mathcal{O}}(g_{m-3} - g_3) = -2$. 由于 h_{m-3}, h_3 的首项系数分别为 -1, $\frac{1}{27}$, 为此我们分以下两种情况加以讨论：

- 当 $p \neq 7$ 时，有 $l(h_{m-3}) \neq l(h_3)$, 因此 $\mathrm{ord}_{\mathcal{O}}\lambda = -1$ 且其首项系数为

$$
\frac{-1 - \frac{1}{27}}{1 - \frac{1}{9}} = -\frac{7}{6}.
$$

在 g_m 的表示式中考虑在 $\mathcal{O}$ 处阶等于 -2 的项，则有

$$
l(g_m) = -l(g_{m-3}) - l(g_3) + l(\lambda)^2
$$

$$
\begin{aligned}
&= -1 - \frac{1}{9} + \frac{49}{36} \\
&= \frac{1}{4} \\
&= \frac{1}{m^2}, \\
l(h_m) &= -l(\lambda)(l(g_m) - l(g_3)) - l(h_3) \\
&= \frac{7}{6}\left(\frac{1}{4} - \frac{1}{9}\right) - \frac{1}{27} \\
&= \frac{1}{8} \\
&= \frac{1}{m^3}.
\end{aligned}
$$

- 当 $p = 7$ 时，有 $l(h_{m-3}) - l(h_3) = -\frac{28}{27} = 0$，因此 λ 在 $\mathcal{O}$ 点处正则. 在 g_m，h_m 的表示式中分别考虑阶等于 -2，-3 的项，则有

$$
\begin{aligned}
l(g_m) &= -l(g_{m-3}) - l(g_3) \\
&= -1 - \frac{1}{9} = -\frac{10}{9} = \frac{1}{4} = \frac{1}{m^2}, \\
l(h_m) &= -l(h_3) = -\frac{1}{27} = \frac{1}{8} = \frac{1}{m^3}.
\end{aligned}
$$

这样就完成了当 $p \neq 2$, 3 时命题的证明.

当 $p \in \{2,3\}$ 时，如果 $m = 1$，命题显然成立. 当 $p = 3$ 时，由命题 3.42 的证明可知对于 $m = 2$ 命题仍然成立.

6. 当 $p \in \{2,3\}$ 时，假设对于 $m - p$ 命题成立，$m \not\equiv 0 \pmod p$. 下面证明对于 m 命题也成立. 设 α，γ 如命题 3.42 所示，则对 $[m-p]$，$[p]$ 利用加法公式可得

$$
\begin{aligned}
\lambda &= \frac{h_p - h_{m-p}}{g_p - g_{m-p}}, \\
g_m &= -g_{m-p} - g_p + \lambda^2 + a_1\lambda - a_2, \\
h_m &= -\lambda(g_m - g_p) - h_p - (a_1 g_m + a_3).
\end{aligned}
$$

由命题 3.42 知，λ^2，g_p 在 $\mathcal{O}$ 处有 2α 阶极点. 下面我们说明以下事实;

- 当 $p = 3$ 时，$\mathrm{ord}_{\mathcal{O}}(g_m - g_{m-p}) = \alpha - 3$，$l(g_m - g_{m-p}) = \frac{\gamma}{m^3}$;
- 当 $p = 2$ 时，$\mathrm{ord}_{\mathcal{O}}(g_m - g_{m-p}) \geqslant \alpha - 2$.

其证明过程如下：由于 $g_m = -g_{m-p} - g_p + \lambda^2 + a_1\lambda - a_2$，而同时 (g_p, h_p)，(g_{m-p}, h_{m-p}) 满足椭圆曲线方程，由此可得

$$
g_m - g_{m-p} = -2g_{m-p} - g_p + \lambda^2 + a_1\lambda - a_2 = \frac{r}{s},
$$

其中

$$
\begin{aligned}
s =& g_p^2 - 2g_p g_{m-p} + g_{m-p}^2, \\
r =& -(g_p^2 - 2g_p g_{m-p} + g_{m-p}^2)(g_p + 2g_{m-p} + a_2) \\
&+ (h_p^2 - 2h_p h_{m-p} + h_{m-p}^2) + a_1(h_p - h_{m-p})(g_p - g_{m-p}) \\
=& (h_p^2 + a_1 h_p g_p - g_p^3 - a_2 g_p^2) \\
&+ (h_{m-p}^2 + a_1 h_{m-p} g_{m-p} - 2g_{m-p}^3 - a_2 g_{m-p}^2) \\
&+ 3g_p g_{m-p}^2 + 2a_2 g_p g_{m-p} - 2h_p h_{m-p} - a_1 h_p g_{m-p} - a_1 h_{m-p} g_p \\
=& -a_3 h_p + a_4 g_p - a_3 h_{m-p} - g_{m-p}^3 + a_4 g_{m-p} + 2a_6 \\
&+ 3g_p g_{m-p}^2 + 2a_2 g_p g_{m-p} - 2h_p h_{m-p} - a_1 h_p g_{m-p} - a_1 h_{m-p} g_p.
\end{aligned}
$$

要注意在命题 3.42 中我们已经知道 g_p, h_p 在 $\mathcal{O}$ 处的阶及其首项系数，而 g_{m-p}, h_{m-p} 在 $\mathcal{O}$ 处的阶以及首项系数可由归纳假设得到. 由此可知 $\mathrm{ord}_{\mathcal{O}} s = -4\alpha$，而其首项系数为 $\frac{1}{\gamma^4}$. 当 $p = 3$ 时，在 r 的表示式中阶最小的项就是 $-2h_p h_{m-p} = h_p h_{m-p}$，其在 $\mathcal{O}$ 处的阶为 $-3\alpha - 3$ 而首项系数等于 $\frac{1}{\gamma^3(m-p)^3} = \frac{1}{\gamma^3 m^3}$. 当 $p = 2$ 时，该项等于零，而余下的项在 $\mathcal{O}$ 处的阶均大于等于 $-3\alpha - 2$. 由此及命题 2.14 可知以上事实成立.

由于 $\alpha \geqslant p$，因此有 $\mathrm{ord}_{\mathcal{O}}(g_m - g_{m-p}) \geqslant 0$. 由命题 2.14 以及定义 3.40 后的注可知

$$
\mathrm{ord}_{\mathcal{O}} g_m = \mathrm{ord}_{\mathcal{O}} g_{m-p} = -2,\ l(g_m) = l(g_{m-p}) = \frac{1}{(m-p)^2} = \frac{1}{m^2}.
$$

对于 h_m，考虑在 $\mathcal{O}$ 处阶较小的项如下

$$
\begin{aligned}
-\lambda(g_m - g_p) - h_p &= \frac{-(h_p - h_{m-p})(g_m - g_p) - h_p(g_p - g_{m-p})}{g_p - g_{m-p}} \\
&= \frac{-h_p(g_m - g_{m-p}) - h_{m-p} g_p + h_{m-p} g_m}{g_p - g_{m-p}}.
\end{aligned}
$$

其分母在 $\mathcal{O}$ 处的阶为 -2α，而首项系数为 $\frac{1}{\gamma^2}$. 下面证明分子在 $\mathcal{O}$ 处的阶为 $-2\alpha - 3$，而其首项系数为 $\frac{1}{\gamma^2 m^3}$. 由此即可完成对 h_m 的证明. 当 $p = 3$ 时，有

$$
\begin{aligned}
\mathrm{ord}_{\mathcal{O}}(h_p(g_{m-p} - g_m)) &= -2\alpha - 3, \\
\mathrm{ord}_{\mathcal{O}}(h_{m-p} g_m) &= -5,
\end{aligned}
$$

$$\mathrm{ord}_{\mathcal{O}}(h_{m-p}g_p) = -2\alpha - 3.$$

虽然第一、三两项在 $\mathcal{O}$ 点处的阶都是最小的，但是它们的首项系数之和不等于零：

$$l(-h_p(g_m - g_{m-p})) + l(-h_{m-p}g_p) = -\frac{1}{\gamma^3}\cdot\frac{\gamma}{m^3} - \frac{1}{m^3}\cdot\frac{1}{\gamma^2} = \frac{1}{\gamma^2 m^3}.$$

当 $p = 2$ 时，由已经证明的事实可知分子中具有最小阶的项为 $h_{m-p}g_p$，其首项系数等于 $-\frac{1}{\gamma^2 m^3} = \frac{1}{\gamma^2 m^3}$.

这样就完成了命题 3.43 的证明. □

当特征等于 2 或 3 时，利用命题 3.42 所做的准备工作，我们可以得到如下更为一般的结论.

命题3.44 *设 $p \in \{2,3\}$，$m = p^v m'$ 是一个正整数且 $\gcd(p, m') = 1$，则*

$$\mathrm{ord}_{\mathcal{O}} g_m = -2\alpha^v,$$

$$\mathrm{ord}_{\mathcal{O}} h_m = -3\alpha^v,$$

$$e_{[m]} = \alpha^v,$$

其中 α 的定义参见命题 3.42.

证明 我们对 v 进行归纳. 当 $v = 0$ 时，由命题 3.43 和命题 3.35 知该命题成立. 假设当 $m = p^v m'$ 时命题成立，下面证明其对 pm 也成立：

$$\begin{aligned}\mathrm{ord}_{\mathcal{O}} g_{pm} &= \mathrm{ord}_{\mathcal{O}}(g_p \circ [m])\\ &= e_{[m]}\mathrm{ord}_{\mathcal{O}} g_p \quad (\text{引理 } 3.14)\\ &= \alpha^v(-2\alpha) \quad (\text{归纳假设})\\ &= -2\alpha^{v+1}.\end{aligned}$$

同样地可以证明 $\mathrm{ord}_{\mathcal{O}} h_{pm} = -3\alpha^{v+1}$. 由定理 2.26 知，$\frac{X}{Y}$ 是 $\mathcal{O}$ 处的一致化参数，因此

$$e_{[pm]} = \mathrm{ord}_{\mathcal{O}}\left(\frac{X}{Y}\circ[pm]\right) = \mathrm{ord}_{\mathcal{O}}\left(\frac{g_{pm}}{h_{pm}}\right) = \alpha^{v+1}.$$ □

不难证明在命题 3.44 的假设条件下，当 $p = 2$ 时，g_m, h_m 的首项系数如下所示：

	$j \neq 0$	$j = 0$
$l(g_m)$	$\dfrac{1}{a_1^{2(2^v-1)}}$	$\dfrac{1}{a_3^{\frac{2}{3}(4^v-1)}}$
$l(h_m)$	$\dfrac{1}{a_1^{3(2^v-1)}}$	$\dfrac{1}{a_3^{4^v-1}}$

由于在本书中我们并不会用到该结论，因此在这里我们并不给出其证明.

下面考虑 $g_m - g_n$ 的除子，其中 m, n 满足某些特定要求. 记 $\langle E[m]\rangle$ 表示只有在 $E[m]$ 中的点处系数等于 1，而在其他点处系数等于零的除子.

命题3.45　*设 m, n 是非零整数.*

- *如果 $p \neq 2$, 3 且 m, n, $m+n$, $m-n$ 都与 p 互素，则*

$$\operatorname{div}(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle.$$

- *如果 $p \in \{2,3\}$, $\gcd(m,p) = 1$, $n = p^v n'$, 其中 $v \geqslant 1$, $\gcd(n',p) = 1$, 则*

$$\operatorname{div}(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\alpha^v\langle E[n]\rangle,$$

其中 α 的定义参见命题 3.42.

证明　为减少篇幅，在这里我们只给出当 $p \in \{2,3\}$ 时命题的证明. 其他情况时的证明与此是非常类似的，具体证明留给读者. (也可参见 [Charlap and Robbins, 1988], Theorem 7.7, p.39.) 首先要注意由于 $E[m]$, $E[n]$ 中的点恰好分别就是 g_m, g_n 中的极点，因此 $g_m - g_n$ 只在 $E[m] \cup E[n]$ 中有极点. 同时又由于 $(g_m - g_n)(P) = 0$ 意味着 $X(mP) = X(nP)$, 也就是 $mP = \pm nP$, 所以 $g_m - g_n$ 只有在 $E[m+n] \cup E[m-n]$ 中才有零点. 由此可知要证明命题成立，只需要确定 $g_m - g_n$ 在 m, n, $m+n$ 和 $m-n$ 扭点处的阶即可. 设 $P \in E[m] \cup E[n] \cup E[m+n] \cup E[m-n]$.

1. 当 $P = \mathcal{O}$ 时，由命题 3.43 及命题 3.44 可知

$$\operatorname{ord}_{\mathcal{O}} g_m = -2, \operatorname{ord}_{\mathcal{O}} g_n = -2\alpha^v < -2.$$

因此 $\operatorname{ord}_{\mathcal{O}}(g_m - g_n) = -2\alpha^v$.

2. 当 $P \in (E[m] \cap E[n]) \backslash \{\mathcal{O}\}$ 时，有 $P \in E[m+n] \cap E[m-n]$. 我们只要证明

$$\operatorname{ord}_P(g_m - g_n) = 1 + 1 - 2 - 2\alpha^v = \operatorname{ord}_{\mathcal{O}}(g_m - g_n)$$

即可. 由于 g_m, g_n 在由 $E[m] \cap E[n]$ 中点构成的平移映射下是不变的，因此

$$\begin{aligned}\operatorname{ord}_P(g_m - g_n) &= \operatorname{ord}_P((g_m - g_n) \circ \tau_{-P}) \\ &= e_{\tau_{-P}}(P)\operatorname{ord}_{\tau_{-P}(P)}(g_m - g_n) \qquad (\text{引理}3.14) \\ &= \operatorname{ord}_{\mathcal{O}}(g_m - g_n). \qquad (\text{引理}3.16)\end{aligned}$$

3. 当 $P \in E[m]\backslash E[n]$ 时，有 $P \notin E[m+n] \cup E[m-n]$，因此我们只要证明 $\operatorname{ord}_P(g_m - g_n) = -2$. 由于 g_m 在平移 τ_P 下是不变的且 $\gcd(m,p) = 1$，因此与前面证明类似地可得 $\operatorname{ord}_P g_m = \operatorname{ord}_{\mathcal{O}} g_m = -2$. 同时由于 g_n 在 $P \notin E[n]$ 处正则，因此 $\operatorname{ord}_P(g_m - g_n) = -2$.
4. 当 $P \in E[n]\backslash E[m]$ 时，由命题 3.44 可知

$$\operatorname{ord}_P g_m \geqslant 0, \quad \operatorname{ord}_P g_n = -2\alpha^v,$$

则

$$\operatorname{ord}_P(g_m - g_n) = -2\alpha^v.$$

得证.

下面假设 $P \notin E[m] \cup E[n]$.

5. 当 $P \in E[m-n]\backslash E[m+n]$，即 $mP = nP \neq -nP$ 时，我们要说明 $g_m - g_n$ 在 P 处有 1 阶零点. P 是 $g_m - g_n$ 的零点是显然的，又由于

$$\begin{aligned}D(g_m - g_n) &= m(2h_m + a_1 g_m + a_3) - n(2h_n + a_1 g_n + a_3) \qquad (\text{定理 } 3.27) \\ &= m(2h_m + a_1 g_m + a_3), \qquad (\text{由于 } p \mid n)\end{aligned}$$

因此

$$\begin{aligned}D(g_m - g_n)(P) &= m(2h_m(P) + a_1 g_m(P) + a_3) \\ &= m(2Y + a_1 X + a_3)(mP) \\ &\neq 0;\end{aligned}$$

因为如果 $D(g_m - g_n)(P) = 0$，则由于 $\gcd(m,p) = 1$，因此 $(2Y + a_1 X + a_3)(mP) = 0$，从而 $mP = nP$ 是 2 阶点，与 $nP \neq -nP$ 矛盾. 由此可得 $\operatorname{ord}_P(D(g_m - g_n)) = 0$，则由定理 3.30 可知 $\operatorname{ord}_P(g_m - g_n) = 1$.
6. 当 $P \in E[m+n]\backslash E[m-n]$，即 $mP = -nP \neq nP$ 时，利用相同的方法可以证明 P 是 $g_m - g_n$ 的 1 阶零点.
7. 当 $P \in E[m+n] \cap E[m-n]$，即 $mP = nP$ 是 2 阶点时，显然 P 是 $g_m - g_n$ 的零点. 下面要说明其阶数是 2. 为此我们分别考虑 $p = 2$ 和 $p = 3$ 两种情况：

- 当 $p=3$ 时, 由定理 3.30 知, $\mathrm{ord}_P(g_m-g_n)=2$ 等同于 $\mathrm{ord}_P(D(g_m-g_n))=1$ 及 $\mathrm{ord}_P(D^2(g_m-g_n))=0$.

$$\begin{aligned}
D(g_m-g_n) &= m(-h_m+a_1g_m+a_3), \qquad (\text{如上所示})\\
D(g_m-g_n)(P) &= 0, \qquad (\text{因为 } mP \text{ 是 2 阶点})\\
D^2(g_m-g_n) &= m^2(a_2g_m-a_4+a_1h_m\\
&\quad +a_1(-h_m+a_1g_m+a_3)), \qquad (\text{定理 3.27})\\
D^2(g_m-g_n)(P) &= m^2(a_2g_m-a_4+a_1h_m)(P)\\
&= m^2\frac{\partial E}{\partial X}(mP),
\end{aligned}$$

由于 mP 是 2 阶点，因此 $\dfrac{\partial E}{\partial Y}(mP)=0$. 由于 E 是非奇异的，因此上式不等于 0.

- 当 $p=2$ 时，由定理 3.30 知上面的方法是无效的. 为此我们分别考虑 $a_1g_m+a_3$ 和 $a_1g_n+a_3$:

$$\begin{aligned}
\mathrm{ord}_P(a_1g_m+a_3) &= \mathrm{ord}_P((a_1X+a_3)\circ[m])\\
&= e_{[m]}\mathrm{ord}_{mP}(a_1X+a_3), \qquad (\text{引理 3.14})
\end{aligned}$$

由命题 3.35 知 $e_{[m]}=1$. 同时由于 mP 是 2 阶点，因此有 $\mathrm{ord}_{mP}(a_1X+a_3)=2$, 则 $\mathrm{ord}_P(a_1g_m+a_3)=2$.

$$\begin{aligned}
\mathrm{ord}_P(a_1g_n+a_3) &= e_{[n]}\mathrm{ord}_{nP}(a_1X+a_3)\\
&= \alpha^v\cdot 2 \qquad (\text{命题 3.44})\\
&> 2.
\end{aligned}$$

而由于存在 2 阶点，所以 $a_1\neq 0$, 因此有

$$\mathrm{ord}_P(g_m-g_n)=\mathrm{ord}_P((a_1g_m+a_3)-(a_1g_n+a_3))=2. \qquad \square$$

命题3.46　*如果* $\gcd(m,p)=1$, 则

$$|E[m]|=m^2.$$

证明　在证明过程中记 $d_{m'}=|E[m']|$. 当 $p\neq 2$, 3 时，由定理 2.28 知主除子的次数等于 0, 因此由命题 3.45 知：当 p 与 m', n', $m'+n'$, $m'-n'$ 互素时，有

$$d_{m'+n'}+d_{m'-n'}-2d_{m'}-2d_{n'}=0. \tag{3.19}$$

下面我们对 m 进行归纳. 当 $m=1$, 2 时命题显然成立. 假设当 $r<m$, $p\nmid r$ 时, 有 $d_r=r^2$, 则

1. 当 $m\not\equiv 1,2 \pmod p$ 时, 则在 (3.19) 式中取 $n'=1$, $m'=m-1$ 可得

$$\begin{aligned} d_m &= 2d_{m-1}+2d_1-d_{m-2} \\ &= 2(m-1)^2+2-(m-2)^2 \\ &= m^2. \end{aligned}$$

2. 当 $m\equiv 1 \pmod p$, $m\geqslant p+1$ 时, 由于 $p\geqslant 5$, 因此 $m\not\equiv 2$, $4 \pmod p$. 在 (3.19) 式中取 $n'=2$, $m'=m-2$, 可得

$$\begin{aligned} d_m &= 2d_{m-2}+2d_2-d_{m-4} \\ &= 2(m-2)^2+8-(m-4)^2 \\ &= m^2. \end{aligned}$$

3. 当 $m\equiv 2 \pmod p$, $m\geqslant p+2$ 时, 有 $m\not\equiv 3$, $6 \pmod p$. 在 (3.19) 中取 $n'=3$, $m'=m-3$ 可得

$$\begin{aligned} d_m &= 2d_{m-3}+2d_3-d_{m-6} \\ &= 2(m-3)^2+18-(m-6)^2 \\ &= m^2. \end{aligned}$$

注意在第一种情况中已经证明了 $d_3=9$.

显然若 $p=2$, $m=\pm1$, 或 $p=3$, $m\in\{-2,-1,1,2\}$ 时, 命题是成立的. 当 $p\in\{2,3\}$, $\gcd(m,p)=1$ 时, 在命题 3.45 中取 $n=p$, 可得

$$d_m = 2d_{m-p}+2\alpha d_p-d_{m-2p}.$$

由 α 的定义可知: 无论 j 是否等于零, 总有 $\alpha d_p=p^2$, 因此

$$\begin{aligned} d_m &= 2(m-p)^2+2p^2-(m-2p)^2 \quad (\text{归纳假设}) \\ &= m^2. \end{aligned}$$

□

有了以上这些知识, 现在就可以来证明命题 3.37 和命题 3.38. 我们已经知道当 $\gcd(m,p)=1$ 时 $E[m]$ 的元素个数. 为得到其群结构, 我们需要以下定理, 其证明可参见任意代数教科书.

定理3.47 (交换群基本定理)　设 $G \neq \{0\}$ 是一个交换群, 则存在唯一的正整数 r 以及 $n_1, \cdots, n_r \geqslant 2$, 满足 $n_i | n_{i+1}$, $i = 1, \cdots, r-1$, 且

$$G \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}.$$

命题 3.37 的证明　我们对 m 的素因子个数进行归纳. 要注意此时 $|E[m]| = m^2$.

1. 当 $m = q$ 是一个素数时, 由定理 3.47 知 $E[q] \simeq \mathbb{Z}_q \times \mathbb{Z}_q$, 或 $E[q] \simeq \mathbb{Z}_{q^2}$ 是循环群. 但是当 $E[q] \simeq \mathbb{Z}_{q^2}$ 时, $E[q]$ 中存在一个阶为 q^2 的元素, 与 $E[q]$ 的定义矛盾.
2. 当 $m = qm'$ 时, 其中 q 是一个素数且 $|m'| > 1$. 由交换群基本定理 3.47, 可设 $E[m] \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, 由 $E[m] = \{P : m'qP = \mathcal{O}\}$ 以及 $[q]$ 是一个满射 (参见命题 3.3) 可知

$$\begin{aligned} E[m'] &= \{P : m'P = \mathcal{O}\} \\ &= \{qP : m'qP = \mathcal{O}\} \\ &= \{qP : P \in E[m]\} \\ &= qE[m]. \end{aligned}$$

由此可得

$$\begin{aligned} E[m'] &\simeq q\mathbb{Z}_{n_1} \times \cdots \times q\mathbb{Z}_{n_r} \\ &\simeq \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{b_r}, \end{aligned}$$

其中

$$b_i = \begin{cases} n_i, & q \nmid n_i, \\ \dfrac{n_i}{q}, & q \mid n_i, \end{cases}$$

且由 $n_i \mid n_{i+1}$ 可得 $b_i \mid b_{i+1}$. 由对 m' 的归纳假设以及 b_i 的唯一性知

$$b_1 = \cdots = b_{r-2} = 1, \quad b_{r-1} = b_r = m',$$

因此

$$n_1 = \cdots = n_{r-2} = q, \quad n_{r-1} = n_r = qm' = m,$$

由此即可得 $m^2 = |E[m]| = q^{r-2}m^2$, 则 $r = 2$, 即 $E[m] \simeq \mathbb{Z}_m \times \mathbb{Z}_m$.　□

为证明命题 3.38，我们需要以下引理.

引理3.48 *p 扭点的个数小于 p^2.*

证明 当 $p \in \{2,3\}$ 时，我们在命题 3.41 中已经看到该引理是成立的. 对于一般的情况，我们将在 3.6 节中利用除子多项式证明该引理. □

命题 3.38 的证明 由引理 3.48 知 $E[p] = \{\mathcal{O}\}$，或者 $E[p] \simeq \mathbb{Z}_p$. 当 $E[p] \simeq \mathbb{Z}_p$ 时，我们对 v 进行归纳证明. 假设 $E[p^{v-1}] \simeq \mathbb{Z}_{p^{v-1}}$，考虑群同态

$$\rho : E[p^v] \to E[p^{v-1}], \quad P \mapsto pP,$$

也就是 $[p]$ 在 $E[p^v]$ 上的限制. 由于 $[p]$ 是一个满射，且 p^{v-1} 扭点在 $[p]$ 下的原象必定是 p^v 扭点，因此 ρ 是一个满射. 其核为 $E[p]$，因此

$$|E[p^v]| = |\operatorname{Im}\rho||\ker\rho| = p^{v-1}p = p^v.$$

由归纳假设知存在 p^{v-1} 阶点 Q，则 Q 在 ρ 下的原象是 p^v 阶点，因此 $E[p^v]$ 必定是一个循环群. □

为了从命题 3.37 和命题 3.38 得到定理 3.39，我们需要以下引理：

引理3.49 *若 $\gcd(m,n)=1$，则 $E[mn] \simeq E[m] \times E[n]$.*

证明 该引理的证明类似于中国剩余定理的证明. 由 Euclidian 算法可知存在整数 e, f 满足 $em + fn = 1$. 定义如下的群同态：

$$\iota : E[m] \times E[n] \to E[mn], \quad (P,Q) \mapsto P + Q,$$

$$\pi : E[mn] \to E[m] \times E[n], \quad P \mapsto (fnP, emP).$$

容易验证 ι, π 的定义是合理的且满足同态的性质. 更进一步地，有 $\pi\circ\iota = \mathrm{id}|_{E[m]\times E[n]}$, $\iota \circ \pi = \mathrm{id}|_{E[mn]}$：

$$\begin{aligned}
\pi \circ \iota(P,Q) &= (fn(P+Q), em(P+Q)) \\
&= (fnP, emQ) \quad (\text{因为 } Q \in E[n], P \in E[m]) \\
&= ((fn+em)P, (fn+em)Q) \\
&= (P,Q), \\
\iota \circ \pi(P) &= (fn+em)P = P.
\end{aligned}$$

□

定理 3.39 的证明 由引理 3.49 知，对于 $m = p^v m'$，$p \nmid m'$，有

$$E[m] \simeq E[m'] \times E[p^v].$$

若 $E[p] = \{\mathcal{O}\}$，则 $E[p^v] = \{\mathcal{O}\}$，因此

$$E[m] \simeq E[m'] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m'}.$$

否则由中国剩余定理知

$$E[m] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m'} \times \mathbb{Z}_{p^v} \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m}.$$

□

3.6 除子多项式

到目前为止，我们都是通过考察有理函数 g_m，h_m 的极点来研究 m 扭点. 但是对它们的零点我们并不十分清楚，而且至少当 $\gcd(m,p)=1$ 时，其极点是否为二阶也不清楚. 在本节中我们通过定义一个只在 m 扭点处有 1 阶零点，且只在无穷远点 $\mathcal{O}$ 处有极点的有理函数来研究它们的零点. 如果这样的有理函数是存在的，则由命题 2.34 知其必是一个多项式. 由于 E 是和 $\mathrm{Pic}^0(E)$ 同构的 (参见推论 2.47)，所以如果 m 扭点之和等于 $\mathcal{O}$，则满足要求的多项式必定存在. 特别地，当 $\gcd(m,p)=1$ 时，这样的多项式一定存在：因为此时对于任意的 m 扭点 P，其逆 $\overline{P}$ 也是 m 扭点，因此所有阶不是 2 的 m 扭点之和必等于 $\mathcal{O}$. 如果 $E[m]$ 中包含 2 阶点，则 m 必定为偶数，且 $E[2] \subseteq E[m]$. 再假定 $p \neq 2$ (参见定义 2.12 后的说明). 在这种情况下有 3 个 2 阶点，并且它们的和等于 $\mathcal{O}$(因为存在一个以 $\langle E[2]\rangle - 4\langle\mathcal{O}\rangle$ 为除子的有理函数，即直线 $2Y + a_1X + a_3$).

为避免特征为正数时所带来的麻烦，我们首先考察特征是零的情况，然后通过模 p 进行约化来说明当 $p > 0$ 时，所得结论依然成立.

除特别说明的以外，以下均假设 $p = 0$.

定义3.50 对于整数 $m \neq 0$，称唯一以 $\langle E[m]\rangle - m^2\langle\mathcal{O}\rangle$ 为除子且首项系数等于 m 的有理函数是 m 次除子多项式，记为 ψ_m. 约定记 $\psi_0 = 0$.

命题3.51 对于正整数 m，n，有以下等式成立：

1. $\psi_{-m} = -\psi_m$；
2. $\psi_m^2 = m^2 \prod\limits_{P\in E[m]\setminus\{\mathcal{O}\}} (X - X(P))$；

3. $\psi_m \in \begin{cases} K[X], & m\text{是奇数}, \\ (2Y + a_1X + a_3)K[X], & m\text{是偶数}; \end{cases}$

4. 如果 m, n 的奇偶性相同，则 $\psi_m\psi_n \in K[X]$.

证明

1. 由于 $E[m] = E[-m]$，因此由定义 3.50 知 $\psi_{-m} = -\psi_m$ 显然成立.
2. 由 $\operatorname{div}(X - X(P)) = \langle P\rangle + \langle \overline{P}\rangle - 2\langle \mathcal{O}\rangle$ 知，式子两边的有理函数具有相同的除子. 同时显然这两个有理函数的首项系数均为 m^2，因此由推论 2.35 知等式必定成立.
3. 若 m 是一个奇数，则 $E[m]$ 不包含 2 阶点，因此 $E[m]$ 可分解为 $E[m] = S \dot{\cup} \overline{S} \dot{\cup} \{\mathcal{O}\}$，其中 $\overline{S} = \{\overline{P} : P \in S\}$. 利用与第 2 点证明相同的方法可得 $\psi_m = m\prod\limits_{P\in S}(X - X(P))$. 若 m 是一个偶数，则 $E[2] \subseteq E[m]$，因此 $E[m]$ 可分解为 $E[m] = S \dot{\cup} \overline{S} \dot{\cup} E[2]$，从而 $\psi_m = \dfrac{m}{2}\psi_2\prod\limits_{P\in S}(X - X(P))$. 由本节开始的讨论可知 $\psi_2 = 2Y + a_1X + a_3$，因此第 3 点成立.
4. 如果 m, n 都是奇数，则由上面第 3 点可知结论成立. 如果 m, n 都是偶数，同样地由第 3 点可知，只需证明 $\psi_2^2 \in K[X]$ 即可：

$$\begin{aligned}
\psi_2^2 &= (2Y + a_1X + a_3)^2 \\
&= 4Y^2 + 4Y(a_1X + a_3) + (a_1X + a_3)^2 \\
&= 4(X^3 + a_2X^2 + a_4X + a_6) + (a_1X + a_3)^2 \\
&\in K[X].
\end{aligned}$$

□

命题3.52 当 m, $n \neq 0$ 时，有

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}.$$

证明 由命题 3.45 知上式两边具有相同的除子. 同时由命题 3.43 知左式的首项系数为 $\dfrac{1}{m^2} - \dfrac{1}{n^2}$，而由定义知右式的首项系数为$-\dfrac{(m+n)(m-n)}{m^2n^2}$，因此左右两式的首项系数也相同，从而等式必定成立. □

命题3.53 除子多项式是唯一满足以下递推关系的多项式：

$\psi_0 = 0,$

$\psi_1 = 1,$

$$\psi_2 = 2Y + a_1Y + a_3,$$
$$\psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,$$
$$\frac{\psi_4}{\psi_2} = 2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2),$$

其中 b_i 的意义参见定义 2.7,

$$\psi_{m+n}\psi_{m-n} = \psi_n^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1}. \tag{3.20}$$

更进一步地有

$$\psi_{2m} = \frac{\psi_m}{\psi_2}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \tag{3.21}$$
$$= (\psi_2 \circ [m])\psi_m^4, \tag{3.22}$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1}. \tag{3.23}$$

证明 当 $m,\ n \neq 0$ 时, 由命题 3.52 及

$$g_m - g_n = (g_m - g_1) - (g_n - g_1)$$

可知

$$\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} = \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2},$$

因此有

$$\psi_{m+n}\psi_{m-n} = \psi_n^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1}.$$

而当 $m = 0$ 或 $n = 0$ 时上式显然成立, 因此 (3.20) 式成立.

对于 ψ_0, ψ_1, ψ_2 公式是显然成立的. 在命题 3.52 中取 $m = 2$, $n = 1$ 可得

$$\psi_3 = -(g_2 - X)\psi_2^2.$$

将 g_2 及 ψ_2 代入上式即可知对于 ψ_3 公式也成立. 类似地由命题 3.52 可知

$$\psi_4 = -\frac{(g_3 - X)\psi_3^2}{\psi_2}.$$

同样可以证明对 ψ_4 公式成立.

为证明唯一性, 我们在 (3.20) 中取特殊的 m, n. 令 $n = 0$ 可得

$$-\psi_m^2\psi_{-1} = \psi_m^2,$$

从而有 $\psi_{-1}=-1$. 再令 $m=0$ 可得

$$-\psi_n^2=\psi_n\psi_{-n},$$

因此 $\psi_{-n}=-\psi_n$. 最后对于 $m\geqslant 3$，取 $n=2$ 则可递归地得到

$$\psi_{m+2}=\frac{\psi_2^2\psi_{m+1}\psi_{m-1}-\psi_m^2\psi_3}{\psi_{m-2}}.$$

因此利用 (3.20) 及 ψ_0，ψ_1，ψ_2，ψ_3 和 ψ_4 就可以唯一确定除子多项式.

在 (3.20) 式中用 $m+1$，$m-1$ 分别代替 m，n 即可得 (3.21). 而取 m，n 分别为 $m+1$，m 即可得 (3.23). 对于 (3.22)，我们计算除子如下：

$$\begin{aligned}
\operatorname{div}\psi_{2m}&=\langle E[2m]\rangle-4m^2\langle\mathcal{O}\rangle,\\
\operatorname{div}\psi_m^4&=4\langle E[m]\rangle-4m^2\langle\mathcal{O}\rangle,\\
\operatorname{div}(\psi_2\circ[m])&=\operatorname{div}([m]^*(\psi_2))\\
&=[m]^*(\operatorname{div}\psi_2)\qquad(\text{命题}3.13)\\
&=[m]^*(\langle E[2]\rangle-4\langle\mathcal{O}\rangle)\\
&=\sum_{P\in[m]^{-1}(E[2])}\langle P\rangle-4\langle E[m]\rangle\\
&=\langle E[2m]\rangle-4\langle E[m]\rangle,
\end{aligned}$$

因此 ψ_{2m}，$(\psi_2\circ[m])\psi_m^4$ 具有相同的除子. 下面再比较它们的首项系数：

$$\begin{aligned}
l(\psi_{2m})&=2m,\\
l((\psi_2\circ[m])\psi_m^4)&=l(2h_m+a_1g_m+a_3)m^4\\
&=\frac{2}{m^3}m^4\qquad(\text{命题}3.43)\\
&=l(\psi_{2m}),
\end{aligned}$$

因此 $\psi_{2m}=(\psi_2\circ[m])\psi_m^4$. □

推论3.54 对任意的 m，有

$$\psi_m\in\mathbb{Z}[X,\ Y,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6]/(E),$$

进一步地，当 m 是奇数时

$$\psi_m\in\mathbb{Z}[X,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6]/(E),$$

当 m 是偶数时

$$\frac{\psi_m}{\psi_2} \in \mathbb{Z}[X,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6]/(E).$$

证明　在命题 3.51 第 4 点的证明中，我们已经得到 $\psi_2^2 \in \mathbb{Z}[X,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6]/(E)$. 下面我们对 m 进行归纳. 当 $m=1,\ 3$ 时是显然的. 而当奇数 $m \geqslant 5$ 时，由 (3.23) 式知推论必定成立. 对于 $m=2k$，只要利用 (3.21) 式对 k 是偶数或奇数分别加以考虑即可. □

下面考虑在可能的情况下，如何利用除子多项式来计算 h_m. 由 (3.21) 及 (3.22) 式可知

$$\begin{aligned} 2h_m + a_1 g_m + a_3 &= \psi_2 \circ [m] \\ &= \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{\psi_2\psi_m^3}. \end{aligned}$$

当特征不等于 2 时，利用上式就可以求出 h_m. 对于特征等于 2 的情况，我们采用 [Koblitz, 1991] 中建议的方法，所得的结论对于任意的特征都是成立的.

命题3.55　设 m 是一个正整数，则可以用以下两种方式表示 h_m:

1.

$$h_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{2\psi_2\psi_m^3} - \frac{1}{2}(a_1 g_m + a_3).$$

2.

$$h_m - Y = \frac{\psi_{m-2}\psi_{m+1}^2}{\psi_2\psi_m^3} - (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{m-1}\psi_{m+1}}{\psi_2\psi_m^2} + \psi_2 \circ [m]$$

或等价地有

$$h_m - Y = \frac{\psi_{m-1}^2\psi_{m+2}}{\psi_2\psi_m^3} - (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{m-1}\psi_{m+1}}{\psi_2\psi_m^2}.$$

证明　由前面的说明可知第 1 点是成立的. 下面利用归纳法来证明第 2 点中的第一个等式. 记

$$s' = -(3X^2 + 2a_2X + a_4 - a_1Y).$$

当 $m=1,\ 2$ 时，通过简单的计算可以证明等式是成立的. 当 $m>2$ 时，由于

$$h_m = -\frac{h_{m-1} - Y}{g_{m-1} - X}(g_m - X) - (a_1 g_m + a_3 + Y),$$

因此

$$h_m - Y = -\frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) - \psi_2 \circ [m] + 2(h_m - Y)$$

$$\Longleftrightarrow h_m - Y = \frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) + \psi_2 \circ [m].$$

由归纳假设及命题 3.52 可得

$$\frac{g_m - X}{g_{m-1} - X}(h_{m-1} - X) = \frac{\psi_{m+1}\psi_{m-1}^3}{\psi_m^3\psi_{m-2}}\left(\frac{\psi_m^2\psi_{m-3}}{\psi_2\psi_{m-1}^3} + s'\frac{\psi_m\psi_{m-2}}{\psi_2\psi_{m-1}^2} + \psi_2 \circ [m-1]\right),$$

又由 (3.21), (3.22) 可知

$$\psi_2 \circ [m-1] = \frac{\psi_{m+1}\psi_{m-2}^2 - \psi_{m-3}\psi_m^2}{\psi_2\psi_{m-1}^3},$$

因此

$$\begin{aligned}\frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) &= \frac{\psi_{m+1}\psi_{m-3}}{\psi_2\psi_{m-2}\psi_m} + s'\frac{\psi_{m+1}\psi_{m-1}}{\psi_2\psi_m^2} + \frac{\psi_{m+1}^2\psi_{m-2}}{\psi_2\psi_m^3} - \frac{\psi_{m+1}\psi_{m-3}}{\psi_2\psi_{m-2}\psi_m}\\ &= \frac{\psi_{m+1}^2\psi_{m-2}}{\psi_2\psi_m^3} + s'\frac{\psi_{m+1}\psi_{m-1}}{\psi_2\psi_m^2},\end{aligned}$$

因此对于 m，该等式成立.

而要证明第 2 点中的第二个等式，只需把 $\psi_2 \circ [m]$ 用 (3.21) 和 (3.22) 式代入即可. □

以下假设特征 p 是任意的.

在推论 3.54 中我们看到：当特征是 0 时，除子多项式的系数均属于 $\mathbb{Z}$. 当特征为 p 时，我们通过模 p 约化来得到相应的除子多项式. 由推论 3.54 知，我们在特征为零时得到的等式属于整环

$$\mathbb{Z}[X,\ Y,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6]/(E)$$

的分式域 (假设此时分母模 p 不为零)，所以我们前面在特征是零时得到的等式仍然成立. 为此我们必须证明以下的引理.

引理3.56 当 $m \neq 0$ 时，$\psi_m \neq 0$.

证明 我们对 $m > 0$ 进行归纳. 对于 ψ_1 引理成立是显然的. 而对于 $\psi_2 = 2Y + a_1X + a_3$，即使当特征等于 2 时，由于 $a_1X + a_3$ 不等于零，因此命题依然成立. 对于一般情况，我们在命题 3.52 中分别取 m, n 为 $m-1$, 1，可得

$$\psi_m\psi_{m-2} = (X - g_{m-1})\psi_{m-1}^2.$$

由归纳假设知 ψ_{m-2}，$\psi_{m-1} \neq 0$，以及当 $m > 2$ 时有 $X \neq g_{m-1}$，因此 $\psi_m \neq 0$. □

下面我们说明除子多项式即使在特征是正数时，依然“保持”其除子. 要不然，这样新定义的除子多项式就没有多大意义.

命题3.57　当 $\gcd(m,p)=1$ 时，

$$\operatorname{div}\psi_m=\langle E[m]\rangle-m^2\langle\mathcal{O}\rangle.$$

证明　当特征等于零时，ψ_m 在无穷远点 $\mathcal{O}$ 处有 m^2-1 阶极点且首项系数等于 m. 由于 $\gcd(m,p)=1$，因此模 p 约化时，首项系数仍然不等于零，因此当特征是 p 时，在无穷远点 $\mathcal{O}$ 处仍然有 m^2-1 阶极点. 由此可知在考虑重数的情况下，ψ_m 共有 m^2-1 个零点. 同时由于在等式

$$g_m-X=-\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2}$$

中，g_m-X 正好以 $E[m]$ 中的点为极点，而 ψ_{m+1}，ψ_{m-1} 没有有限极点，因此 ψ_m 正好以 $E[m]\backslash\{\mathcal{O}\}$ 中的点为有限零点. 由于这样的点的个数是 m^2-1，因此这些零点一定是 1 阶零点，从而命题成立. □

引理 3.48 的证明　由于当进行模 p 约化时，ψ_p 的首项系数等于零，因此 ψ_p 的有限零点的个数小于 p^2-1. 类似于命题 3.57 的证明可知 $E[p]\backslash\{\mathcal{O}\}$ 中的点必定是 ψ_p 的零点，则 $|E[p]|<p^2$. □

例　设 $p\in\{2,3\}$，$\gcd(m,p)=1$，$n=p^vn'$，其中 $v\geqslant 1$，$\gcd(n',p)=1$，则由命题 3.45 知

$$\operatorname{div}(g_m-g_n)=\langle E[m+n]\rangle+\langle E[m-n]\rangle-2\langle E[m]\rangle-2\alpha^v\langle E[n]\rangle.$$

同时

$$g_m-g_n=-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2},$$

其中 m，$m+n$，$m-n$ 与 p 互素. 由此可得

$$\operatorname{div}\psi_n=\alpha^v\langle E[n]\rangle-\alpha^v|E[n]|\langle\mathcal{O}\rangle,$$

所以 ψ_n 在 $E[n]$ 的有限点处有 α^v 阶零点.

3.7　Weil 对

前面我们通过检查 m 扭点所得到的只是“局部”信息，而我们感兴趣的是“椭圆曲线上有多少个点的坐标在有限域中”这样一个“全局”的信息. Weil 对就可以

完成从局部到全局的转化. 实际上 Weil 对可以看成是 m 扭点的 "双线性" 形式, 具体含义参见 3.8 节.

在本节中, m 表示与 p 互素的正整数.

在定义 Weil 对和介绍其性质之前, 我们首先引入一个引理. 该引理反映了自同态 $[m]$ 和域扩张 $K(E)/[m]^*(K(E))$ 性质之间的联系.

引理3.58 设 r 是一个有理函数, 并且其在由 $E[m]$ 中点构成的平移映射下是不变的, 则存在一个有理函数 s, 使得 $r = s \circ [m]$, 即 $r \in [m]^*(K(E))$.

证明 如果利用 "对于任意一个可分自同态 α, 则域扩张 $K(E)/\alpha^*(K(E))$ 是可分扩张" 这一结论, 通过用 $E[m]$ 代替 $\ker\alpha$ 就可以证明该引理. 但由于我们在前面并没有证明该结论, 所以这里我们采用另外一种证明方法. 实际上我们证明

$$[K(E) : [m]^*(K(E))] \leqslant m^2 = \deg[m]. \tag{3.24}$$

利用 (3.24) 就可以完成引理的证明: 记

$$J = [m]^*(K(E)) = \{t \circ [m] : t \in K(E)\},$$
$$H = \{r \in K(E) : r \circ \tau_S = r, \quad \forall S \in E[m]\},$$

则有 $J \subseteq H \subseteq K(E)$, $[K(E) : H] \leqslant [K(E) : J]$. $\{\tau_S^* : S \in E[m]\}$ 是由 m^2 个 $K(E)$ 域自同构构成的群, 而 H 是其固定域, 因此由 Galois 理论知 $[K(E) : H] = m^2$. 又由 (3.24) 知 $m^2 = [K(E) : H] \geqslant [K(E) : J]$, 即 $[K(E) : J] = [K(E) : H]$, 因此 $H = J$, 即引理成立 (由 Galois 理论还可以得到 $K(E)/J$ 是可分的, 但这一结论我们用不着).

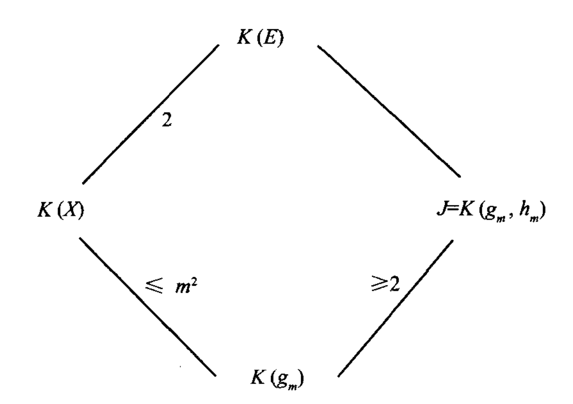
为证明 (3.24), 我们考虑域 $K(g_m)$, $K(g_m, h_m)$, $K(X)$ 和 $K(E)$. 注意

$$J = K(X \circ [m], Y \circ [m]) = K(g_m, h_m).$$

由命题 3.51 知 ψ_m^2, $\psi_{m-1}\psi_{m+1} \in K[X]$, 则由命题 3.52 知 (取 $n = 1$):

$$g_m - X = -\frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \in K(X),$$

因此 $g_m \in K(X)$, $K(g_m) \subseteq K(X)$(这反映了 mP 与 $m\overline{P} = \overline{mP}$ 的 X 坐标是相同的, 而与 P 的 Y 坐标无关). 下面说明扩域的次数满足以下关系:



其中 $[K(E):K(X)]=2$ 是已经知道的. 考虑 $[K(X):K(g_m)]$, 由命题 3.52 知 X 满足以下 $K(g_m)[T]$ 中的多项式:

$$f(T):=T\psi_m^2(T)-(\psi_{m-1}\psi_{m+1})(T)-g_m\psi_m^2(T).$$

当特征等于零时, ψ_m^2 在 $\mathcal{O}$ 点有 $2(m^2-1)$ 阶极点, 因此由引理 2.31 知其次数等于 m^2-1; $\psi_{m-1}\psi_{m+1}$ 在 $\mathcal{O}$ 点有 $(m-1)^2+(m+1)^2-2=2m^2$ 阶极点, 所以其次数等于 m^2, 因此 $\deg f\leqslant m^2$. 当特征大于零时, 除子多项式的次数只可能降低, 因此同样有 $\deg f\leqslant m^2$, 所以有 $[K(X):K(g_m)]\leqslant m^2$. 再说明 $h_m\notin K(g_m)$, 否则有 $h_m\in K(X)$, 从而对任意的 $P\in E$, 有

$$Y(mP)=h_m(P)=h(\overline{P})=Y(\overline{mP}).$$

而当 mP 不是 2 阶点时, 上式显然并不成立, 所以 $[K(g_m,h_m):K(g_m)]\geqslant 2$, 因此有

$$[K(E):J]=\frac{[K(E):K(X)][K(X):K(g_m)]}{[J:K(g_m)]}\leqslant\frac{2m^2}{2}=m^2.\qquad\square$$

下面定义 Weil 对. 本节余下的部分与文献 [Charlap and Robbins, 1988] 第 12 节中的 61~68 页是一样的.

对于 m 扭点 T, 定义 g_T 是满足 $\operatorname{div} g_T=[m]^*(\langle T\rangle-\langle\mathcal{O}\rangle)$ 的有理函数. 首先我们说明这样的定义是合理的 . 由于 $\deg([m]^*(\langle T\rangle-\langle\mathcal{O}\rangle))=0$, 且又由命题 3.3 知, $[m]$ 是 E 上的满射, 因此存在点 T_0 满足 $[m]T_0=T$, 因此有

$$\begin{aligned}[m]^*(\langle T\rangle-\langle\mathcal{O}\rangle)&=\sum_{T\in[m]^{-1}(T)}\langle T'\rangle-\sum_{R\in\ker[m]}\langle R\rangle\\&=\sum_{R\in E[m]}(\langle T_0+R\rangle-\langle R\rangle).\end{aligned}$$

对此显然有

$$\sum_{R \in E[m]} (T_0 + R - R) = m^2 T_0 = mT = \mathcal{O},$$

即构成除子的点之和等于无穷远点 $\mathcal{O}$, 因此由推论 2.47 知 $[m]^*(\langle T \rangle - \langle \mathcal{O} \rangle)$ 是主除子, 所以满足要求的有理函数 g_T 是存在的.

定义3.59 m 扭点的 Weil 对就是函数

$$e_m : E[m] \times E[m] \to \mu, \quad (S, T) \mapsto \frac{g_T \circ \tau_S}{g_T},$$

其中 μ 表示 K 中 m 次单位根所构成的集合.

由于以 $[m]^*(\langle T \rangle - \langle \mathcal{O} \rangle)$ 为除子的有理函数只相差一个非零常数因子, 因此 $e_m(S, T)$ 与 g_T 的选取是无关的. 同时由于

$$\begin{aligned}
\operatorname{div}(g_T \circ \tau_S) &= \tau_S^*(\operatorname{div} g_T) \qquad (\text{命题 } 3.13) \\
&= \tau_S^* \left(\sum_{R \in E[m]} (\langle T_0 + R \rangle - \langle R \rangle) \right) \\
&= \sum_{R \in E[m]} (\langle T_0 + R - S \rangle - \langle R - S \rangle) \\
&= \operatorname{div} g_T,
\end{aligned}$$

因此 $e_m(S, T) \in K$. 而在本节的最后将证明 $e_m(S, T)^m = 1$.

命题3.60 Weil 对具有以下性质:

1. "双线性性": 对任意的 S, S_1, S_2, T, T_1, $T_2 \in E[m]$, 有

$$e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T),$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2);$$

2. "恒等性": 对任意的 $S \in E[m]$, 有

$$e_m(S, S) = 1;$$

3. "交错性": 对任意的 S, $T \in E[m]$, 有

$$e_m(S, T) = e_m(T, S)^{-1};$$

4. “非退化性”

$$e_m(S,T)=1,\quad \forall S\in E[m]\Longleftrightarrow T=\mathcal{O},$$
$$e_m(S,T)=1,\quad \forall T\in E[m]\Longleftrightarrow S=\mathcal{O};$$

5. “相容性”：设 α 是一个非零自同态，则

$$e_m(\alpha(S),\alpha(T))=e_m(S,T)^{\deg\alpha}.$$

证明

1. 由于

$$\begin{aligned}e_m(S_1+S_2,T)&=\frac{g_T\circ\tau_{S_1+S_2}}{g_T}=\frac{g_T\circ\tau_{S_1}\circ\tau_{S_2}}{g_T}\\&=\left(\frac{g_T\circ\tau_{S_1}}{g_T}\circ\tau_{S_2}\right)\frac{g_T\circ\tau_{S_2}}{g_T}\\&=(e_m(S_1,T)\circ\tau_{S_2})e_m(S_2,T)\\&=e_m(S_1,T)e_m(S_2,T),\quad (e_m(S_1,T)\text{ 是一个常数})\end{aligned}$$

因此双线性性中的第一个等式成立. 为证明第二个等式，需要把 $g_{T_1+T_2}$ 与 g_{T_1}，g_{T_2} 相联系. 由于 $\langle T_1+T_2\rangle-\langle T_1\rangle-\langle T_2\rangle+\langle\mathcal{O}\rangle$ 是主除子，因此存在有理函数 h，满足

$$\operatorname{div}h=\langle T_1+T_2\rangle-\langle T_1\rangle-\langle T_2\rangle+\langle\mathcal{O}\rangle,$$

则

$$\begin{aligned}\operatorname{div}\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}&=[m]^*(\langle T_1+T_2\rangle-\langle T_1\rangle-\langle T_2\rangle+\langle\mathcal{O}\rangle)\\&=[m]^*(\operatorname{div}h)\\&=\operatorname{div}(h\circ[m]),\qquad(\text{命题 3.13})\end{aligned}$$

因此

$$\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}=ch\circ[m],$$

在由 $E[m]$ 中点构成的平移映射下是不变的，其中 $c\in K^\times$. 由此可得

$$\begin{aligned}e_m(S,T_1+T_2)&=\left(\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\circ\tau_S\right)\frac{(g_{T_1}\circ\tau_S)(g_{T_2}\circ\tau_S)}{g_{T_1+T_2}}\\&=\frac{g_{T_1}\circ\tau_S}{g_{T_1}}\cdot\frac{g_{T_2}\circ\tau_S}{g_{T_2}}\\&=e_m(S,T_1)e_m(S,T_2).\end{aligned}$$

2. 设 $S_0 \in E$ 满足 $mS_0 = S$. 考察 $g_S \circ \tau_{iS_0}$ 并令

$$G := \prod_{i=0}^{m-1} (g_S \circ \tau_{iS_0}).$$

则

$$\begin{aligned}
\operatorname{div}(g_S \circ \tau_{iS_0}) &= \tau_{iS_0}^*(\operatorname{div} g_S) \quad (\text{命题 } 3.13)\\
&= (\tau_{iS_0}^* \circ [m]^*)(\langle S\rangle - \langle \mathcal{O}\rangle)\\
&= ([m] \circ \tau_{iS_0})^*(\langle S\rangle - \langle \mathcal{O}\rangle) \quad (\text{命题 } 3.15)\\
&= (\tau_{iS} \circ [m])^*(\langle S\rangle - \langle \mathcal{O}\rangle)\\
&= [m]^*(\langle S - iS\rangle - \langle -iS\rangle),\\
\operatorname{div} G &= [m]^*\left(\sum_{i=0}^{m-1}(\langle (1-i)S\rangle - \langle (0-i)S\rangle)\right)\\
&= [m]^*\left(\sum_{i=2-m}^{1}\langle iS\rangle - \sum_{i=1-m}^{0}\langle iS\rangle\right)\\
&= [m]^*(\langle S\rangle - \langle S - mS\rangle)\\
&= 0. \quad (\text{因为 } mS = \mathcal{O})
\end{aligned}$$

因此由命题 2.34 以及推论 2.33 可知 G 是一个常数，且有

$$\begin{aligned}
1 &= \frac{G \circ \tau_{S_0}}{G}\\
&= \frac{g_S \circ \tau_{mS_0}}{g_S \circ \tau_{0S_0}}\\
&= \frac{g_S \circ \tau_S}{g_S}\\
&= e_m(S,S).
\end{aligned}$$

3. 由直接计算即可证明“交错性”成立：

$$\begin{aligned}
1 &= e_m(S+T, S+T)\\
&= e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T) \qquad (\text{双线性性})\\
&= e_m(S,T)e_m(T,S). \qquad (\text{恒等性})
\end{aligned}$$

4. 由“交错性”知只需证明第一个式子即可. 如果 $T = \mathcal{O}$, 则 g_T 是一个常数，从而在平移映射下是不变的，因此 $e(S,T) = 1$. 假设对任意的 $S \in E[m]$, 有

$e_m(S,T)=1$，即 g_T 在由 m 扭点构成的平移映射下是不变的，因此由引理 3.58 知，存在某个有理函数 r，使得 $g_T = r\circ[m]$. 由于

$$\begin{aligned}[m]^*(\langle T\rangle-\langle \mathcal{O}\rangle) &= \operatorname{div} g_T\\ &= \operatorname{div}(r\circ[m])\\ &= [m]^*\operatorname{div} r, \quad (\text{命题 } 3.13)\end{aligned}$$

则由 $[m]^*$ 是一个单射可知 $\operatorname{div} r = \langle T\rangle-\langle \mathcal{O}\rangle$. 因为 r 没有有限极点，因此其是一个多项式. 又由于 r 只有一个零点，因此其必定是一个常数 (参见命题 2.34 以及推论 2.33)，从而 $\operatorname{div} r = 0$，$T=\mathcal{O}$.

5. 设 T 是某个固定的 m 扭点. 下面证明对任意的 m 扭点 S，有

$$\frac{g_{\alpha(T)}\circ\tau_{\alpha(S)}}{g_{\alpha(T)}} = \left(\frac{g_T\circ\tau_S}{g_T}\right)^{\deg\alpha}$$

由于左式是一个常数，因此可以和 α 进行复合而不改变它的值：

$$\begin{aligned}\frac{g_{\alpha(T)}\circ\tau_{\alpha(S)}}{g_{\alpha(T)}} &= \frac{g_{\alpha(T)}\circ\tau_{\alpha(S)}\circ\alpha}{g_{\alpha(T)}\circ\alpha}\\ &= \frac{g_{\alpha(T)}\circ\alpha\circ\tau_S}{g_{\alpha(T)}\circ\alpha}.\end{aligned}$$

右式为

$$\left(\frac{g_T\circ\tau_S}{g_T}\right)^{\deg\alpha} = \frac{g_T^{\deg\alpha}\circ\tau_S}{g_T^{\deg\alpha}}.$$

因此我们只要证明对任意的 m 扭点 S，有

$$\frac{g_{\alpha(T)}\circ\alpha}{g_T^{\deg\alpha}}\circ\tau_S = \frac{g_{\alpha(T)}\circ\alpha}{g_T^{\deg\alpha}}.$$

由引理 3.58 知其等价于证明存在某个有理函数 r，使得

$$\frac{g_{\alpha(T)}\circ\alpha}{g_T^{\deg\alpha}} = r\circ[m].$$

由于

$$\begin{aligned}\operatorname{div}\left(\frac{g_{\alpha(T)}\circ\alpha}{g_T^{\deg\alpha}}\right) &= (\alpha^*\circ[m]^*)(\langle\alpha(T)\rangle-\langle\mathcal{O}\rangle)-\deg\alpha[m]^*(\langle T\rangle-\langle\mathcal{O}\rangle)\\ &= [m]^*(\alpha^*(\langle\alpha(T)\rangle-\langle\mathcal{O}\rangle)-\deg\alpha(\langle T\rangle-\langle\mathcal{O}\rangle))\end{aligned}$$

$$= [m]^* \left(\sum_{R \in \ker \alpha} e_\alpha(\langle T+R \rangle - \langle R \rangle) - \deg \alpha(\langle T \rangle - \langle \mathcal{O} \rangle) \right),$$

因此只要证明括号中的除子是主除子即可. 显然该除子的次数等于零，且有

$$\begin{aligned} \sum_{R \in \ker \alpha} e_\alpha(T+R-R) - \deg \alpha(T - \mathcal{O}) &= (e_\alpha |\ker \alpha| - \deg \alpha)T \\ &= \mathcal{O}. \quad (\deg \alpha \text{ 的定义}) \end{aligned}$$

□

最后我们证明 $e_m(S,T)$ 是 m 次单位根：

$$\begin{aligned} e_m(S,T)^m &= e_m(S, mT) \quad (\text{双线性性}) \\ &= e_m(S, \mathcal{O}) \\ &= 1. \end{aligned}$$

3.8 Hasse 定理

现在我们可以证明著名的 Hasse 定理. 在 [Hasse, 1934] 中，Hasse 对特征为奇数的情况给出了相应的证明.

定理3.61 (Hasse 定理) *设 $k = \mathbb{F}_q$, $t = q + 1 - |E_k|$, 则 Frobenius 自同态 φ 满足:*

1. $\varphi \circ \varphi - [t] \circ \varphi + [q] = [0]$,
2. $|t| \leqslant 2\sqrt{q}$.

这里的证明与 [Charlap and Robbins, 1988] 第 12 节中 69~72 页中的证明是一致的. 为了行文的完整性这里给出了该定理的证明. 利用前面几节中所得到的结论，该定理的证明很大程度上就是线性代数中的问题. 注意在命题 3.37 中，我们已经证明了：对于与 p 互素的整数 m, $E[m] \simeq \mathbb{Z}_m \times \mathbb{Z}_m$ 是一个秩为 2 的自由 $\mathbb{Z}_m$ 模.

引理3.62 *设 $\{T_1, T_2\}$ 是 $E[m]$ 作为 $\mathbb{Z}_m$ 模的一组基，则 $e_m(T_1, T_2)$ 是 m 次本原单位根.*

证明 为证明 $e_m(T_1, T_2)$ 是 m 次本原单位根，只要证明 $e_m(T_1, T_2)$ 的阶为 m 即可. 由上节可知

$$e_m(T_1, T_2)^m = 1,$$

因此只要证明 m 是满足 $e_m(T_1,T_2)^m=1$ 的最小正整数即可，即如果 $e_m(T_1,T_2)^n=1$，则 $m\mid n$. 假设 $e_m(T_1,T_2)^n=1$，则对 $c_1,c_2\in\mathbb{Z}_m$，有

$$\begin{aligned}
e_m(nT_1,c_1T_1+c_2T_2)&=e_m(T_1,c_1T_1+c_2T_2)^n \quad (\text{命题 3.60 中的第 1 条})\\
&=e_m(T_1,T_1)^{nc_1}e_m(T_1,T_2)^{nc_2} \quad (\text{命题 3.60 中的第 2 条})\\
&=1. \quad (\text{命题 3.60 中的第 1 条})
\end{aligned}$$

由于 $\{T_1,T_2\}$ 是一组基，因此 $E[m]$ 中的元素都可以表示为 $c_1T_1+c_2T_2$ 的形式. 由 e_m 的 “非退化性”(命题 3.60 中的第 4 条) 可得 $nT_1=\mathcal{O}$，因此 $m|n$. □

下一个定理将自同态的整体信息与将其限制到 $E[m]$ 上得到的局部信息相联系. 在该定理的证明中将应用到 Weil 对.

定理3.63 *设 α 是一个非零自同态，则 α 在 $E[m]$ 上的限制 (记为 α_m) 是一个线性自同态，且其行列式的值是 $\deg\alpha \pmod m$.*

证明 显然 $\alpha(E[m])\subseteq E[m]$，$\alpha_m$ 是线性的. 由此知 α_m 作为 $\mathbb{Z}_m$ 模 $E[m]$ 上的自同态定义是合理的. 设 $\{T_1,T_2\}$ 是 $E[m]$ 的一组基，则 α_m 可以用矩阵

$$A=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$$

来表示，其中 $\alpha_m(T_j)=a_{1j}T_1+a_{2j}T_2$. 由计算可得

$$\begin{aligned}
e_m(T_1,T_2)^{\deg\alpha}&=e_m(\alpha(T_1),\alpha(T_2)) \quad (\text{命题 3.60 中的第 5 条})\\
&=e_m(a_{11}T_1+a_{21}T_2,a_{12}T_1+a_{22}T_2)\\
&=e_m(T_1,T_1)^{a_{11}a_{12}}e_m(T_1,T_2)^{a_{11}a_{22}}e_m(T_2,T_1)^{a_{21}a_{12}}e_m(T_2,T_2)^{a_{21}a_{22}}\\
&=e_m(T_1,T_2)^{a_{11}a_{22}-a_{21}a_{12}}\\
&=e_m(T_1,T_2)^{\det\alpha_m}.
\end{aligned}$$

由引理 3.62 知 $e_m(T_1,T_2)$ 是 m 次本原单位根，因此

$$\deg\alpha=\det\alpha_m \pmod m.$$ □

下面我们要确定两个自同态的线性组合的次数.

命题3.64 *设 α, β 是两个非零自同态，c_1, $c_2\in\mathbb{Z}$，则*

$$\deg([c_1]\circ\alpha+[c_2]\circ\beta)=c_1^2\deg\alpha+c_2^2\deg\beta+c_1c_2(\deg(\alpha+\beta)-\deg\alpha-\deg\beta).$$

证明 设 m 是大于左、右两式的整数并且 $\gcd(m,p)=1$. 所有的自同态 $\mathrm{End}(E)$ 可以看作一个 $\mathbb{Z}$ 模. 把所有自同态都限制到 $E[m]$ 上得到的集合记为 $\mathrm{End}(E)\mid_{E[m]}$, 则其就是一个 $\mathbb{Z}_m$ 模. 而这两个模是相容的, 即对于任意的 $\alpha\in\mathrm{End}(E)$ 以及任意的 $c\in\mathbb{Z}$, $c\alpha$ 在 $E[m]$ 上的限制恰好就等于 $(c \mod m)\alpha_m$, 即

$$([c]\circ\alpha)_m = c\alpha_m,$$

因此由定理 3.63 可得

$$\deg([c_1]\circ\alpha+[c_2]\circ\beta)=\det(c_1\alpha_m+c_2\beta_m) \pmod{m}.$$

通过对 2×2 矩阵的简单计算可得

$$\begin{aligned}\det(c_1\alpha_m+c_2\beta_m)=&c_1^2\det\alpha_m+c_2^2\det\beta_m\\&+c_1c_2(\det(\alpha_m+\beta_m)-\det\alpha_m-\det\beta_m).\end{aligned}$$

再次利用定理 3.63 可知命题 3.64 成立. □

命题3.65 设 α 是一个自同态, 则

$$\beta:=\alpha\circ\alpha-[1+\deg\alpha-\deg([1]-\alpha)]\circ\alpha+[\deg\alpha]=[0].$$

证明 和前面一样, 我们把所有的自同态限制到 $E[m]$ 上, 其中 $\gcd(m,p)=1$, 则

$$\beta_m=\alpha_m^2-(1+\det\alpha_m-\det(\mathrm{id}-\alpha_m))\alpha_m+\det\alpha_m.$$

再次通过对 2×2 矩阵的简单计算可得

$$\mathrm{Tr}\alpha_m=1+\det\alpha_m-\det(\mathrm{id}-\alpha_m),$$

因此由 Cayley-Hamilton 定理可知 $\beta_m=0$. 通过改变 m, 可知对无限多个扭点 P, 有 $\beta(P)=\mathcal{O}$, 因此 $\beta=[0]$; 否则有 $\beta=(\beta_1,\beta_2)$, 而 β_i 只有有限多个极点. □

Hasse 定理的证明 由于 k 是 $x\mapsto x^q$ 的固定域, 因此

$$\begin{aligned}E_k&=\{(x,y)\in E:(x^q,y^q)=(x,y)\}\cup\{\mathcal{O}\}\\&=\{P\in E:\varphi(P)=P\}\\&=\ker([1]-\varphi).\end{aligned}$$

由推论 3.36 可知 $[1]-\varphi$ 是可分的，即 $e_{[1]-\varphi}=1$，因此

$$\deg([1]-\varphi)=|\ker([1]-\varphi)|=|E_k|.$$

由定义 3.20 后的例题可知 $\deg\varphi=q$，则在命题 3.65 中取 $\alpha=\varphi$ 可知 Hasse 定理的第一部分成立.

对任意的 c_1，$c_2\in\mathbb{Z}\backslash\{0\}$，由命题 3.64 可得

$$c_1^2+c_2^2q-c_1c_2t=\deg([c_1]\circ[1]+[c_2]\circ(-\varphi))>0,$$

两边除以 c_2^2 可得

$$\left(\frac{c_1}{c_2}\right)^2-\frac{c_1}{c_2}t+q\geqslant 0,$$

即

$$r^2-rt+q\geqslant 0,\quad \forall r\in\mathbb{Q}.$$

因此该不等式在 $\mathbb{R}$ 上成立，其判别式 $t^2-4q\leqslant 0$，即 $t^2\leqslant 4q$. □

3.9　Weil 定理

在特殊的情况下，椭圆曲线上点的个数是比较容易计算的：设 $L=\mathbb{F}_{q^m}$ 是 $k=\mathbb{F}_q$ 的 m 次扩域且 $|E_k|$ 是已知的，则 $|E_L|$ 可由公式得出. 特别地，如果 k 比较小，则可以通过检查所有可能的 X，Y 坐标来确定 $|E_k|$. 这样的曲线经常应用于密码学中，例如文献 [Koblitz, 1991], p.158 中提及的 $\mathbb{F}_{2^m}$ 上的椭圆曲线

$$Y^2+XY=X^3+X^2+1.$$

设 $s=q+1-|E_k|$，$t=q^m+1-|E_L|$，则由 Hasse 定理知

$$\varphi_k:(x,y)\mapsto(x^q,y^q)$$

是多项式

$$T^2-sT+q\in\mathbb{Z}[T]$$

在 $\mathrm{End}(E)$ 中的零点. 同样地，$\varphi_L:(x,y)\mapsto(x^{q^m},y^{q^m})$ 是 T^2-tT+q^m 的零点. 更进一步地，如果 $t'\neq t$，则 φ_L 必定不是 $T^2-t'T+q^m$ 的零点：否则由

$$\varphi_L\circ\varphi_L+[q^m]=[t]\circ\varphi_L,$$

$$\varphi_L\circ\varphi_L+[q^m]=[t']\circ\varphi_L,$$

可得 $[0]=[t'-t]\circ\varphi_L$. 由命题 3.3 知 φ_L 是一个满射，因此 $[t'-t]=[0]$，进而有 $t'=t$. 同时由于 $\varphi_L=\varphi_k^m$，所以由上可知 t 是使 φ_k 是 $T^{2m}-tT^m+q^m$ 零点的唯一整数.

为构造这样的多项式，我们考虑 T^2-sT+q 的复零点 α, β. 由 Hasse 定理知该二次多项式的判别式 $D=s^2-4q$ 不可能为正数，因此 α, β 是两个共轭的复根. 同时 α, β 也是虚二次数域 $\mathbb{Q}(\sqrt{D})$ 中的代数整数，即它们属于 $\mathbb{Z}[v]$，其中

$$v=\begin{cases}\sqrt{D}, & D\not\equiv 1 \pmod 4,\\ \dfrac{1+\sqrt{D}}{2}, & D\equiv 1 \pmod 4,\end{cases}$$

考虑多项式

$$f(T)=T^{2m}-(\alpha^m+\beta^m)T^m+q^m.$$

由于 α, β 是共轭的复根，因此 $\alpha^m+\beta^m$ 是一个实数，因此 $\alpha^m+\beta^m\in\mathbb{Z}[v]\cap\mathbb{R}=\mathbb{Z}$，所以 $f\in\mathbb{Z}[T]$. 更进一步地，由于 $\alpha\beta=q$，所以

$$f(\alpha)=\alpha^{2m}-(\alpha^m+\beta^m)\alpha^m+q^m=-\alpha^m\beta^m+q^m=0.$$

同样地，有 $f(\beta)=0$. 当 $D<0$ 时，α, β 是 f 两个不同的复根，因此在 $\mathbb{Z}[T]$ 中 $T^2-sT+q=(T-\alpha)(T-\beta)$ 整除 f. 由此可知 φ_k 是 f 的零点. 当 $D=0$ 时，只要说明 $\alpha=\beta$ 是 f 的 2 重根，从而以上的结论也成立. 此时，α 为

$$f'(T)=2mT^{m-1}(T^m-\alpha^m)$$

的零点，因此 f 在 α 处有阶至少为 2 的零点.

这样我们就证明了下面的定理：

定理3.66 (Weil) *设 E 是定义在 $\mathbb{F}_q$ 上的椭圆曲线，$|E_{\mathbb{F}_q}|=q+1-s$，而 m 是一个正整数. 在复数域上分解 $T^2-sT+q=(T-\alpha)(T-\beta)$，则*

$$|E_{\mathbb{F}_{q^m}}|=q^m+1-(\alpha^m+\beta^m).$$

例 设 $Y^2+Y=X^3+X+1$ 是定义在 $\mathbb{F}_2$ 上的椭圆曲线；将 $\mathbb{F}_2$ 中的元素 0, 1 代入 X, Y 可得该方程总是不成立的，即 $E_{\mathbb{F}_2}=\{\mathcal{O}\}$，因此 $s=2$. 由于

$$T^2-2T+2=(T-(1+i))(T-(1-i)),$$

因此

$$|E_{\mathbb{F}_{2^m}}|=2^m+1-((1+i)^m+(1-i)^m)=2^m+1-\begin{cases}2\cdot(-4)^{\frac{m}{4}}, & m\equiv 0 \pmod 4,\\ 0, & m\equiv 2 \pmod 4,\\ 2\cdot(-4)^{\frac{m-1}{4}}, & m\equiv 1 \pmod 4,\\ (-4)^{\frac{m+1}{4}}, & m\equiv 3 \pmod 4.\end{cases}$$

当 $m=2$ 时，可得 $|E_{\mathbb{F}_4}|=5$. 这与推论 2.48 后例题所得的结果是一致的.

译者注　事实上，利用 Weil 定理计算 $|E_{\mathbb{F}_{q^m}}|$ 时，并不需要求解方程 T^2-sT+q，而只需利用 Locus 序列递归计算即可，详见 [IEEE, 1998] 附录 A 中的算法 A.11.5.

3.10　挠　曲　线

如果已经知道 $k=\mathbb{F}_q$ 上椭圆曲线 E_k 的点数，则可以构造出另一条曲线 E'_k，使得 E'_k 上的点数也是容易确定的. 具体而言，构造出的椭圆曲线 E'_k 满足：设 k_1，k'_1 分别表示 E_k，E'_k 上点的 X 坐标所构成的集合，则在 k_1，$k\backslash k'_1$ 之间存在一一对应. 由此可以证明当 $|E_k|=q+1-t$ 时，有 $|E'_k|=q+1+t$. 首先我们考察对于一个给定 $x\in k$，何时其是 E_k 上某一点的 X 坐标，也就是考察二次方程 $E(x,Y)$ 何时在 k 中有解.

命题3.67　*设 $Y^2+aY+b\in k[Y]$ 是一个二次方程.*

1. *当 $p\neq 2$ 时，该方程在 k 中有解的充要条件是以下等价论断之一成立：*
   - *a^2-4b 等于零，或者其是 k 中的二次剩余.*
   - *$\gcd(Y^2+aY+b,\ Y^q-Y)\neq 1$.*
2. *当 $p=2$ 时，记*

$$\mathrm{Tr}: k\to\mathbb{F}_2,\quad x\mapsto\sum_{i=0}^{m-1}x^{2^i}$$

为 k 的绝对迹函数，则该二次方程在 k 中有解的充要条件是

$$a=0\quad 或\quad \mathrm{Tr}(a^{-2}b)=0.$$

证明

1. 由于

$$\sigma: k^\times\to k^\times,\quad x\mapsto x^2$$

是乘法群同态，且其核是 $\{\pm1\}$，因此 σ 的象集是 $k^\times$ 中指数为 2 的子群. 该象集中的元素就称为是二次剩余，而 $k^\times\backslash\sigma(k^\times)$ 中的元素就称为是二次非剩余 .

令

$$\chi: k^\times \to \{\pm 1\}, \quad x \mapsto \begin{cases} 1, & x \text{ 是二次剩余}, \\ -1, & x \text{ 是二次非剩余}. \end{cases}$$

再令 $\chi(0)=0$, 则 χ 是 k 上的积性函数. 由

$$Y^2+aY+b=\left(Y+\frac{a}{2}\right)^2-\frac{a^2-4b}{4}$$

可知该二次方程在 k 中有解的充要条件是 $\chi(a^2-4b)\neq -1$. 更进一步地，其在 k 中有 $\chi(a^2-4b)+1$ 个不同的解. 由此知第一个论断成立.

在应用领域最感兴趣的情形是：p 是一个 (大) 素数，$\chi(x)$ 为 Legendre 符号 $\left(\frac{x}{p}\right)$(其利用二次互反律就可以有效地计算. 参见 [Gauβ, 1801], Article 131, [Koblitz, 1994], Chapter II.2). 在更一般的情况下，由于

$$Y^q-Y=\prod_{y\in k}(Y-y),$$

因此

$$\gcd(Y^2+aY+b, Y^q-Y)=\prod_{y\in k: y^2+ay+b=0}(Y-y),$$

由此可知第二个论断成立.

2. 由于 $x\mapsto x^2$ 是 $k=\mathbb{F}_{2^m}$ 上的自同构，因此当 $a=0$ 时，论断显然成立. 当 $a\neq 0$ 时，可以通过作用变换 $Y\mapsto aY$, 并将得到的方程约去 a^2, 使 Y 的系数为 1. 因此不妨设 $a=1$. 设 $y\in k$ 是 $Y^2+Y=b$ 的根，则由逐次平方可得

$$y^{2^i}+y^{2^{i-1}}=b^{2^{i-1}},\quad 1\leqslant i\leqslant m.$$

将以上得到的等式相加得到

$$0=y^{2^m}+y=\mathrm{Tr}b,$$

因此给定的条件是必要的.

注意到如果 y 是 $Y^2+Y=b$ 的根，则 $y+1$ 就是该方程的另外一个根，即根是成对出现的. 因此所有在 k 中有解的方程 $Y^2+Y=b$ 必形如 $(Y+y)(Y+y+1)$, $y\in k$, 从而这样方程的个数恰是所有形如 $Y^2+Y=b$ 方程个数的一半. 另一方面，由上面的讨论知在 k 中有解的方程必定满足 $\mathrm{Tr}b=0$, 而满足该条件的方程的个数也恰好等于所有方程个数的一半，因此论断成立. □

为构造曲线 E'，我们首先考虑 $p \neq 2$ 的情况. 假设 E 为标准形式的椭圆曲线：$Y^2 = s(X)$，其中

$$s(X) = X^3 + a_2X^2 + a_4X + a_6,$$

则由命题 3.67 的证明过程可得

$$\begin{aligned}
|E_k| &= |E_k \backslash \{\mathcal{O}\}| + 1 \\
&= \sum_{x \in k} (\chi(s(x)) + 1) + 1 \\
&= q + 1 + \sum_{x \in k} \chi(s(x)) \\
&= q + 1 + t,
\end{aligned}$$

其中 $t = \sum_{x \in k} \chi(s(x))$.

对于固定的二次非剩余 $\gamma \in k$，定义椭圆曲线 $E' : Y^2 = s'(X)$，其中

$$s'(X) = X^3 + \gamma a_2 X^2 + \gamma^2 a_4 X + \gamma^3 a_6,$$

则 $s'(\gamma x) = \gamma^3 s(x)$，因此

$$\begin{aligned}
|E'_k| &= q + 1 + \sum_{x \in k} \chi(s'(x)) \\
&= q + 1 + \sum_{x \in k} \chi(s'(\gamma x)) \\
&= q + 1 + \chi(\gamma)^3 \sum_{x \in k} \chi(s(x)) \\
&= q + 1 - t,
\end{aligned}$$

当 $p = 2$ 时，我们考虑一般的椭圆曲线

$$E : Y^2 + (a_1X + a_3)Y = s(X),$$

其中

$$s(X) = X^3 + a_2X^2 + a_4X + a_6, \ a_1X + a_3 \neq 0.$$

由命题 3.67 可知

$$\begin{aligned}
|E_k| &= |E_k \backslash E[2]| + |E_k \cap E[2]| \\
&= 2|\{x \in k : a_1x + a_3 \neq 0, \mathrm{Tr}((a_1x + a_3)^{-2} s(x)) = 0\}| + |E_k \cap E[2]|.
\end{aligned}$$

由 2.5 节知

$$E[2] \subseteq E_k$$

且

$$|E[2]| = \begin{Bmatrix} 1 & a_1 = 0 \\ 2 & a_1 \neq 0 \end{Bmatrix} = |\{x \in k : a_1x + a_3 = 0\}| + 1.$$

设 $\gamma \in k$，且 $\mathrm{Tr}\gamma = 1$，令椭圆曲线 E' 为

$$Y^2 + (a_1X + a_3)Y = s'(X),$$

其中

$$s'(X) = s(X) + \gamma(a_1X + a_3)^2,$$

则

$$\begin{aligned}\mathrm{Tr}((a_1x + a_3)^{-2}s'(x)) &= \mathrm{Tr}((a_1x + a_3)^{-2}s(x) + \gamma) \\ &= \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) + 1,\end{aligned}$$

因此

$$\begin{aligned}|E_k| + |E'_k| =&2|\{x \in k : a_1x + a_3 \neq 0, \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) = 0\}| \\ &+ 2|\{x \in k : a_1x + a_3 \neq 0, \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) = 1\}| \\ &+ 2|E[2]| \\ =&2|\{x \in k : a_1x + a_3 \neq 0\}| + 2(|\{x \in k : a_1x + a_3 = 0\}| + 1) \\ =&2(q + 1).\end{aligned}$$

因此当 $|E_k| = q + 1 + t$ 时，$|E'_k| = q + 1 - t$.

由上可知有下面的命题成立：

命题3.68 设 E 是 k 上的椭圆曲线，定义椭圆曲线 E' 如下：

1. 若 $p \neq 2$，$E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$，$\gamma$ 是 k 中的二次非剩余，则令

$$E' : Y^2 = X^3 + \gamma a_2X^2 + \gamma^2 a_4X + \gamma^3 a_6.$$

2. 若 $p = 2$，$E : Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6$，$\gamma \in k$ 且 $\mathrm{Tr}\gamma = 1$，则令

$$E' : Y^2 + (a_1X + a_3)Y = X^3 + (a_2 + \gamma a_1^2)X^2 + a_4X + (a_6 + \gamma a_3^2).$$

E' 被称为是由 γ 确定的 E 的挠曲线. 若 $|E_k| = q + 1 + t$，则 $|E'_k| = q + 1 - t$.

注意：如果 E' 是 E 的挠曲线 (由 γ 确定)，那么 E 也是 E' 的挠曲线. 具体地说，当 $p \neq 2$ 时，E 是由 γ^{-1} 确定的 E' 的挠曲线；当 $p = 2$ 时，E 是由 γ 确定的 E' 的挠曲线，即挠曲线的定义是 "对称" 的. 但是需要注意的是 E 的挠曲线并不是唯一的：由于当 $p \neq 2$ 时，存在着 $\frac{q-1}{2}$ 个二次非剩余，而当 $p = 2$ 时，存在着 $\frac{q}{2}$ 个迹为 1 的元素，因此 E 存在着 $\frac{q-1}{2}\left(\text{或 } \frac{q}{2}\right)$ 条不同的挠曲线. 下面的命题说明虽然 E 的挠曲线并不是唯一的，但这些挠曲线本质上是一样的.

命题3.69　*设 E 是 k 上的椭圆曲线，则 E 由二次非剩余或迹是 1 的元素确定的挠曲线在 k 上是同构的，即挠曲线定义了椭圆曲线 k 同构类上的一个双射.*

这里 "在 k 上同构" 是指存在着系数属于 k 的容许的变量变换，其将某一条挠曲线变换为另一条挠曲线，参见 2.3 节.

证明

1. 设 $p \neq 2, E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$. 对于 E 由二次非剩余确定的两条不同的挠曲线，其中一条曲线可以看成是另一条曲线由二次剩余确定的 "挠曲线"，因此只要证明：如果 $\gamma = \delta^2$ 是 k 中的二次剩余，则 $E'' : Y^2 = X^3 + \gamma a_2X^2 + \gamma^2 a_4X + \gamma^3 a_6$ 与 E 同构即可. 由于容许的变量变换

$$(X, Y) \mapsto (\gamma^{-1}X, (\gamma\delta)^{-1}Y)$$

将 E 变换为 E''，因此上面的结论显然成立.

2. 设 $p = 2$, $E : Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6$，我们要证明对于迹等于零的元素 γ,

$$E'' : Y^2 + (a_1X + a_3)Y = X^3 + (a_2 + \gamma a_1^2)X^2 + a_4X + (a_6 + \gamma a_3^2)$$

与 E 同构.

由于 $\mathrm{Tr}\gamma = 0$，因此由命题 3.67 知二次方程

$$s^2 + a_1s + \gamma a_1^2 = 0,$$
$$t^2 + a_3t + \gamma a_3^2 = 0,$$

在 k 中有解 s, t. 由于容许的变量变换

$$(X,\ Y) \mapsto (X,\ Y + sX + t)$$

将 E 变换为 $E'' + (a_3 s + a_1 t)X$，因此只要证明 $a_3 s + a_1 t = 0$ 即可. 由 s, t 的定义可知

$$(a_3 s + a_1 t)^2 = a_1 a_3 (a_3 s + a_1 t),$$

因此当 $a_3 s + a_1 t \neq 0$ 时，有 $a_3 s + a_1 t = a_1 a_3$. 此时将 s 用 $X^2 + a_1 X + \gamma a_1^2$ 的第二个根 $s' = s + a_1$ 代替，则有 $a_3 s' + a_1 t = (a_3 s + a_1 t) + a_1 a_3 = 0$. □

3.11 超奇异曲线

超奇异曲线是一类特殊的椭圆曲线，其点数以及群结构是非常容易确定的. 在本节中我们将列举有关超奇异曲线的相关性质. 这些性质可以通过函数域以及阿贝尔簇的相关理论来得到. 由于这些内容已经超出了本书所涉及的范围，因此建议有兴趣的读者参阅相关的书籍.

定义3.70 若 $\mathrm{End}(E)$ 是非交换的，则称椭圆曲线 E 是超奇异的.

定理3.71 当 $p = 2, 3$ 时，E 超奇异的充要条件是 $j(E) = 0$.

证明 参见 [Deuring, 1941], 第 253 页和第 255 页. □

Waterhouse 在其博士论文中给出有限域上椭圆曲线点数的所有可能情况 (参见 [Waterhouse, 1969], p.536).

定理3.72 (Waterhouse) 设 $k = \mathbb{F}_q = \mathbb{F}_{p^m}$，$t$ 是满足 $|t| \leqslant 2\sqrt{q}$ 的整数，则在 k 上存在满足 $|E_k| = q + 1 - t$ 的椭圆曲线 E 的充要条件是以下条件之一成立：

1. p, t 互素.

2. m 是偶数，且

- $t = \pm 2\sqrt{q}$,
- $t = \pm\sqrt{q}$, $p \not\equiv 1 \pmod 3$，或
- $t = 0$, $p \not\equiv 1 \pmod 4$.

3. m 是奇数，且

- $t = 0$，或
- $t = \pm\sqrt{pq}$, $p = 2, 3$.

在第一种情况下，椭圆曲线是非超奇异的. 而在余下的两种情况下都是超奇异的.

推论3.73 $k = \mathbb{F}_q$ 上的椭圆曲线 E 为超奇异的充要条件是 $p \mid q + 1 - |E_k|$.

Schoof 指出对于大多数超奇异椭圆曲线，其群结构都可以从其点数中得以确定 (参见 [Schoof, 1987], p.196).

定理3.74 设 E 是定义在有限域 $k=\mathbb{F}_q$ 上的超奇异椭圆曲线，$t=q+1-|E_k|$，则 E_k 的群结构如下所示：

- 当 $t^2\in\{q,\ 2q,\ 3q\}$ 时，E_k 是循环群.
- 当 $t=\pm 2\sqrt{q}$ 时，$E_k\simeq\mathbb{Z}_{\sqrt{q}\mp 1}\times\mathbb{Z}_{\sqrt{q}\mp 1}$.
- 当 $t=0,\ q\not\equiv 1 \pmod 4$ 时，E_k 是循环群；当 $t=0,\ q\equiv 1 \pmod 4$ 时，E_k 是循环群或者 $E_k\simeq\mathbb{Z}_2\times\mathbb{Z}_{\frac{q+1}{2}}$.

在文献 [Schoof, 1987], p.194 中，Schoof 还给出了 t 所对应的非同构椭圆曲线的数目 $N(t)$.

定理3.75 (Schoof) 设 $k=\mathbb{F}_q=\mathbb{F}_{p^m}$ 是一个有限域，记 $N(t)$ 表示 k 上满足 $q+1-|E_k|=t$ 的非同构椭圆曲线 E 的个数. 若 $|t|\leqslant 2\sqrt{q}$，则有

1. 当 t,p 互素时，$N(t)=H(t^2-4q)$.
2. 当 m 是偶数时，

$$
\begin{aligned}
N(\pm 2\sqrt{q}) &= \frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right),\\
N(\pm\sqrt{q}) &= 1-\left(\frac{-3}{p}\right),\\
N(0) &= 1-\left(\frac{-4}{p}\right).
\end{aligned}
$$

3. 当 m 是奇数时，

$$
\begin{aligned}
N(0) &= H(-4p),\\
N(\pm\sqrt{pq}) &= 1, \quad \text{当 } p=2,\ 3 \text{ 时}.
\end{aligned}
$$

这里 $H(\Delta)$ 表示负数 Δ 的 Kronecker 类数 (其定义参见 [Schoof, 1987] 中的第 2 节)，而 $\left(\frac{a}{p}\right)$ 表示 Legendre 符号. 要注意的是 Kronecker 符号只有当 $|\Delta|$ 较小时才能有效计算，所以该定理并不适用于确定较大域上非超奇异曲线同构类的个数. 对于特征为 2, 3 时的超奇异曲线，我们感兴趣的值 $H(-4p)$ 是可以计算的，即有 $H(-8)=1,\ H(-12)=2$.

当特征为偶数时，Menezes 和 Vanstone 给出了定理 3.75 的一个初等证明，并给出了每个同构类的代表元 (参见 [Menezes and Vanstone, 1990]). 表 3.1 给出了 $\mathbb{F}_{2^m}$ 上超奇异曲线的相关结论，其中 m 是偶数，γ 是非立方的，$\omega,\ \alpha,\ \beta,\ \delta\in\mathbb{F}_{2^m}$ 且满足

$$
\mathrm{Tr}\omega=\mathrm{Tr}(\gamma^{-2}\alpha)=\mathrm{Tr}(\gamma^{-4}\beta)=1,\quad \mathrm{Tr}_{\mathbb{F}_4}\delta\neq 0,
$$

这里 $\mathrm{Tr}\kappa = \sum_{i=0}^{m-1} \kappa^{2^i}$ 表示 κ 的绝对迹，$\mathrm{Tr}_{\mathbb{F}_4}\kappa = \sum_{i=0}^{m/2-1} \kappa^{4^i}$ 表示子域 $\mathbb{F}_4$ 上的迹. 在 t 所在的那一列中，当 $\frac{m}{2}$ 是偶数时，取上面的符号；而当 $\frac{m}{2}$ 是奇数时，取下面的符号. 表 3.2 给出了 m 为奇数时的相关结论，其中当 $m \equiv \pm 1 \pmod 8$ 时，取上面的符号；而当 $m \equiv \pm 3 \pmod 8$ 时，取下面的符号.

表 3.1 m 为偶数时，$\mathbb{F}_{2^m}$ 上超奇异曲线的同构类

代表元	t
$Y^2 + \gamma Y = X^3$	$\pm\sqrt{q}$
$Y^2 + \gamma Y = X^3 + \alpha$	$\mp\sqrt{q}$
$Y^2 + \gamma^2 Y = X^3$	$\pm\sqrt{q}$
$Y^2 + \gamma^2 Y = X^3 + \beta$	$\mp\sqrt{q}$
$Y^2 + Y = X^3 + \delta X$	0
$Y^2 + Y = X^3$	$\mp 2\sqrt{q}$
$Y^2 + Y = X^3 + \omega$	$\pm 2\sqrt{q}$

表 3.2 m 为奇数时，$\mathbb{F}_{2^m}$ 上超奇异曲线的同构类

代表元	t
$Y^2 + Y = X^3$	0
$Y^2 + Y = X^3 + X$	$\pm\sqrt{2q}$
$Y^2 + Y = X^3 + X + 1$	$\mp\sqrt{2q}$

同样地，Morain 给出了特征等于 3 时超奇异曲线的同构类 [Morain, 1997]，具体结论参见表 3.3 和 3.4. 其中 γ 是二次非剩余，δ 是绝对迹为 1 的元素. 对于表 3.3(或表 3.4) 来说，当 $\frac{m}{2}$(对于表 3.4 而言 $\frac{m-1}{2}$) 为偶数时取上面的符号，而当 $\frac{m}{2}$(对于表 3.4 而言 $\frac{m-1}{2}$) 为奇数时，取下面的符号.

表 3.3 m 为偶数时，$\mathbb{F}_{3^m}$ 上超奇异曲线的同构类

代表元	t
$Y^2 = X^3 - X$	$\pm 2\sqrt{q}$
$Y^2 = X^3 - \gamma^2 X$	$\mp 2\sqrt{q}$
$Y^2 = X^3 - \gamma X$	0
$Y^2 = X^3 - \gamma^3 X$	0
$Y^2 = X^3 - X + \delta$	$\mp\sqrt{q}$
$Y^2 = X^3 - \gamma^2 X + \gamma^3 \delta$	$\pm\sqrt{q}$

表 3.4　m 为奇数时, $\mathbb{F}_{3^m}$ 上超奇异曲线的同构类

代表元	t
$Y^2 = X^3 + X$	0
$Y^2 = X^3 - X$	0
$Y^2 = X^3 - X + \delta$	$\mp\sqrt{3q}$
$Y^2 = X^3 - X - \delta$	$\pm\sqrt{3q}$

3.12　群　结　构

在确定了 $k = \mathbb{F}_q$ 上椭圆曲线 E 的点数以后, 就需要考虑其群结构. 由交换群基本定理 3.47 可知, E_k 与以下形式的循环群的直积同构, 并且这样的直积是唯一的

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

其中 $n_1 > 1$, $n_i \mid n_{i+1}, i = 1, \cdots, r-1$. 由于 E_k 是有限的, 因此其必定是一个挠群, 从而存在整数 m, 使得 $E_k \subseteq E[m]$. 由定理 3.39 知, 对于恰当的整数 m_1, m_2, $E[m]$ 与 $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ 同构, 因此 $r \leqslant 2$(参见命题 4.2).

定理3.76 (Rück, 1987)　*设 E 是定义在 $\mathbb{F}_q$ 上的椭圆曲线, 则*

$$E_{\mathbb{F}_q} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

其中 $n_1 \mid n_2$, $n_1 \mid q-1$.

注意定理 3.76 包含了椭圆曲线点群是循环群的特殊形式, 此时 $n_1 = 1$.

证明　由前面的讨论可知, 只需证明 $n_1 \mid q-1$ 即可. 下面的证明方法是由 Berit Skjernaa 和 Scott Vanstone 提供的. 由 $n_1 \mid n_2$ 可知 E_k 包含子群 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_1}$, 因此就存在着 n_1^2 个 n_1 扭点. 由定理 3.39 可知, 这就是所有的 n_1 扭点.

下面将利用 Weil 对证明 k 包含 n_1 次本原单位根. 由引理 3.62 以及以上的说明可知, 存在点 $P, Q \in E[n_1] \subseteq E_k$, 使得 $e_{n_1}(P, Q)$ 为 n_1 次本原单位根. 令 φ 为 E_k 的 Frobenius 自同态, 则由 $\varphi(P) = P, \varphi(Q) = Q$ 可得

$$\begin{aligned} e_{n_1}(P,Q) &= e_{n_1}(\varphi(P), \varphi(Q)) \\ &= e_{n_1}(P,Q)^{\deg\varphi} \quad (\text{命题 } 3.60) \\ &= e_{n_1}(P,Q)^q, \quad (\text{参见定义 } 3.20 \text{ 后的例题}). \end{aligned}$$

因此 $e_{n_1}(P, Q) \in k$, 从而 $e_{n_1}(P, Q)$ 的 (乘法) 阶 n_1 必整除 $k^\times$ 的阶 $q-1$.　　□

第 4 章　离散对数问题

第 1 章中介绍的公钥密码体制依赖于特定群中求解离散对数问题的难度：如果攻击者能够很容易地求解密码体制所依赖的离散对数问题，那么攻击者也就能够攻破整个密码体制. 因此为了判断一个密码体制的安全性，我们必须仔细地研究有关求解离散对数的算法.

为了给后面的研究确定一个共同的框架，我们给出离散对数的定义，并约定如下的记号：设 $G=\langle\alpha\rangle$ 是一个有限乘法循环群，α 为其生成元，且 $|G|=n$，$\beta\in G$. 所谓离散对数问题就是确定整数 l(记为 $\log_\alpha\beta$)，使得 $\beta=\alpha^l$. 由于 α 的阶为 n，显然在模 n 的意义下，整数 l 是唯一确定的. 离散对数问题可以利用*一般性算法*或*黑盒算法*(black box) 加以解决. 在这种算法中并不考虑群元素的表示，而只要求能够有效地进行乘法、求逆以及判断两个群元素是否相等这三种运算. 利用这三种基本的运算，对于给定的 α,β，就可以求解离散对数 $\log_\alpha\beta$. 需要注意的是虽然对于大多数群而言，判断两个群元素是否相等是非常简单的，但对于商群来说这却是一个问题，因为商群是由一个群模去一个等价关系得到的，因此商群中同一个元素有多个不同的代表元. 椭圆曲线的除子类群就是这样一个例子. 对于除子类群来说，这个问题可按如下方式解决：每个元素都可唯一地用一个点来表示，即选择除子 $\langle P\rangle-\langle\mathcal{O}\rangle$ 作为代表元 (参见推论 2.44). 其他方面的例子有：数域的类群、一般代数曲线的除子类群等. 在这类群中判断两个元素是否相等就比较麻烦.

实际上，离散对数问题的求解难度在很大程度上取决于群元素的表示. 例如，对于循环群 $G=\mathbb{Z}_n$，$\alpha=1$ 而言，求解任意一个元素的离散对数是非常容易的. 进一步地，即使生成元 $\alpha\neq 1$ 时，利用 Euclidian 算法，也可以方便地求解任意一个元素的离散对数 (实际上 G 中离散对数问题的求解相当于求 G 和 $\mathbb{Z}_n$ 之间一个清晰的同构映射). 由此可见，在寻找解决离散对数问题的有效算法时，应当把群元素的表示方式一并加以考虑. 例如在 4.4 节中我们将会看到对于有限域的乘法群，存在非常有效的算法来求解离散对数. 同时在 4.5 节中我们将利用前几章中的知识，说明某些类型的椭圆曲线对于密码学应用来说是不安全的.

4.1　Shanks's 大步–小步法

Shanks 的大步–小步法基本上就是一个一般性的算法，它近乎求解 α 所有的

幂次以判断其是否等于 β. 但是当采用合适的数据结构以及一定的存储空间时，大步–小步法比穷举法更为有效. 该算法最初是为了计算虚二次数域的类数 [Shanks, 1971]. 该算法的变体可用于确定交换群的结构. 例如在 5.1 节中，我们将介绍的计算椭圆曲线点数的算法.

在大步–小步法中，并不直接计算 $\alpha, \alpha^2, \cdots$ 直至得到 β，而是首先预计算 α 的一系列较小幂次 (“小步”)，然后对于某个正整数 b，计算 $\alpha^b, \alpha^{2b}, \cdots$ 直至某个 α^{ib} 等于预计算中的某个元素 (“大步”). 如果只是通过判断两个元素是否相等来在预计算表中查找 α^{ib}，那么该算法与穷举法相比并没有什么优势. 但是如果每个群元素只有唯一的表示形式并且这些表示是有序的，那么就可以把预计算所得的结果保存在一个有序的数组中，从而利用二分法就可以有效地检索 α^{ib}. 由于大步–小步法应当满足以上要求，因此从理论上讲该算法并不是一个一般性的算法，但是在实践中对于大多数我们感兴趣的群，以上要求都是满足的.

对于有限素域 $\mathbb{F}_p^\times$ 而言，其每个元素都可唯一地表示为 $\{1, \cdots, p-1\}$ 中元素的形式，并显然这样的表示是有序的. 而 $\mathbb{F}_{p^m}^\times$ 中的每个元素都可以唯一表示为 $\mathbb{F}_p[X]$ 中次数小于 m 的多项式形式，并且利用次数以及系数的有序性就可以完成 $\mathbb{F}_{p^m}^\times$ 中元素的排序. 对于椭圆曲线而言，由于我们考察的点属于 $\mathbb{F}_q \times \mathbb{F}_q$，那么就可以利用两个分量的字典排序法来完成椭圆曲线上点的排序.

大步–小步法的具体描述如下：

1. 确定 “小步” 的次数 b.
2. 计算 $(\alpha^i,\ i)$, $0 \leqslant i < b$, 然后按 α^i 的次序对结果加以保存.
3. 取定 “大步” 的次数 $g = \left\lceil \dfrac{n}{b} \right\rceil$.
4. 计算 $\beta\alpha^{-kb}$, $0 \leqslant k < g$, 然后利用二分法在已有关于 α^i 的结果中查询 $\beta\alpha^{-kb}$. 若查询成功，则 $\log_\alpha \beta = kb + i$.

由于 $\log_\alpha \beta \in \{0, \cdots, n-1\}$，因此 $\log_\alpha \beta$ 必可唯一表示为

$$\log_\alpha \beta = kb + i,$$

其中 $0 \leqslant i < b$, $0 \leqslant k < \left\lceil \dfrac{n}{b} \right\rceil$. 由此可知该算法必定可以中止.

在 “小步” 的计算及排序过程中，需 $O(b \log b)$ 次运算，其中一次运算是指一次乘法或两个群元素的一次比较. 而在 “大步” 的计算过程中，需 $O(g \log b)$ 次运算，且两个 O 系数是大体相当的. 因此要确定 (近似) 最优的整数 b，只要考虑 $b+g$ 的最小值即可，其中 $bg = n$. 由此可得 $b = g = \sqrt{n}$. 由于 b, g 均为整数，因此 $b = g = \lceil \sqrt{n}\, \rceil$，从而该算法的复杂度为 $O(\sqrt{n} \log n)$. 同时由于该算法需储存 $\lceil \sqrt{n}\, \rceil$ 个长度为 $O(\log n)$ 的元素，因此其空间复杂度为 $O(\sqrt{n} \log n)$.

要注意的是即使当群中的元素个数 n 未知时，Shanks 方法仍然是适用的：取群元素个数的一个上界，然后运行大步 - 小步法. 即使是当元素个数的上界也无法确定时，此时可任意选取 n，然后运行该算法. 如果此时利用该算法不能求出离散对数，则重新选取更大的 n.

4.2 Pollard's ρ 算法

Shanks 算法的缺点是当群比较大时需要较多的存储空间. 为此 Pollard 提出了概率型算法，其运算时间与 Shanks 算法是大致相同的，但该算法的优势在于其几乎不需要什么存储空间. Pollard 在文献 [Pollard, 1978] 中提出该算法时，考虑的是有限素域的乘法群，但是可以按如下方式推广到任意群上.

设 $G = T_1 \dot\cup T_2 \dot\cup T_3$ 是对 G 的一个随机划分，且每个集合的大小大体上是相当的. 随机选取 a_0，b_0，计算 $x_0 = \alpha^{a_0}\beta^{b_0}$，然后按如下方式递归地定义序列 $(x_i)_{i\geqslant 0}$，$(a_i)_{i\geqslant 0}$，$(b_i)_{i\geqslant 0}$：

$$x_{i+1} = \begin{cases} \beta x_i, & x_i \in T_1, \\ x_i^2, & x_i \in T_2, \\ \alpha x_i, & x_i \in T_3, \end{cases}$$

$$a_{i+1} = \begin{cases} a_i, & x_i \in T_1, \\ 2a_i, & x_i \in T_2, \\ a_i + 1, & x_i \in T_3, \end{cases} \qquad b_{i+1} = \begin{cases} b_i + 1, & x_i \in T_1, \\ 2b_i, & x_i \in T_2, \\ b_i, & x_i \in T_3, \end{cases}$$

则对任意的 $i \geqslant 0$，有 $x_i = \alpha^{a_i}\beta^{b_i}$.

由于 G 是一个有限群，因此序列 (x_i) 最终必定满足周期性，即存在唯一的最小整数 $\mu \geqslant 0$ 以及 $\lambda \geqslant 1$，使得当 $i \geqslant \mu$ 时，$x_{i+\lambda} = x_i$，而 $x_1, \cdots, x_{\mu+\lambda-1}$ 各不相同. 整数 μ 被称为是前周期，而 λ 被称为周期 . 如果将序列中的元素用平面上的点来表示，而将两个连续的元素 x_i，x_{i+1} 用从 x_i 出发指向 x_{i+1} 的直线相连接，则可得图 4.1. 该图形直观上看类似于希腊字母 ρ，这也就是该算法得名的原因.

ρ 算法的关键是寻找匹配 $x_i = x_j$，$i \neq j$. 如果得到满足条件的 x_i，x_j，则

$$\alpha^{a_i+lb_i} = \alpha^{a_i}\beta^{b_i} = x_i = x_j = \alpha^{a_j}\beta^{b_j} = \alpha^{a_j+lb_j},$$

因此

$$l(b_j - b_i) \equiv a_i - a_j \pmod{n}. \tag{4.1}$$

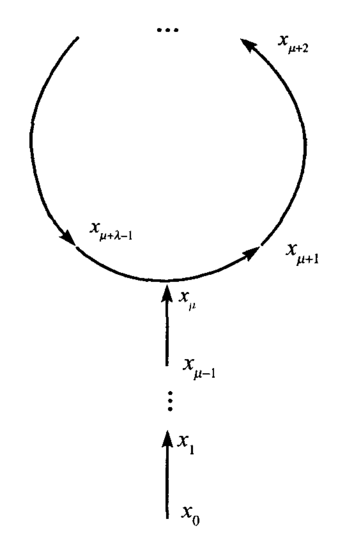


图 4.1 Pollard ρ 算法

若 $d=\gcd(n,b_j-b_i)=1$，则利用 (4.1) 即可求解 l. 否则存在着 d 个可能的 l，则至少当 d 较小时，可以通过检查 $\alpha^l=\beta$ 是否成立，来得到最终的 l. 确切地说，由扩展 Euclidian 算法，可计算得出满足

$$d=un+v(b_j-b_i)$$

的整数 u,v. 在 (4.1) 式两边乘以 v 可得

$$ld\equiv v(a_i-a_j)\pmod n.$$

由 (4.1) 知 $d\mid a_i-a_j$，因此 l 必定是以下 d 个不同值中的某一个

$$\frac{v(a_i-a_j)}{d}+k\frac{n}{d}\pmod n,\quad 0\leqslant k<d.$$

实际上，4.3 节中描述的 Pohlig–Hellman 算法将离散对数问题约化为只需考虑 n 是素数的情况，因此一般来讲 d 并不会非常大.

第一个可能检测到的匹配是 $x_\mu=x_{\mu+\lambda}$，此时需计算 $\mu+\lambda$ 个序列中的元素. 假设映射

$$F:G\to G,\quad x\mapsto\begin{cases}\beta x_i, & x_i\in T_1\\ x_i^2, & x_i\in T_2\\ \alpha x_i, & x_i\in T_3\end{cases}$$

是一个随机映射，即其取值是从所有 $G \to G$ 的映射中完全随机选取的，则 $\mu + \lambda$ 的期望值近似于

$$\sqrt{\frac{\pi}{2}n} \approx 1.25\sqrt{n} \in O(\sqrt{n}),$$

参见 [Teske, 1998].

大量的实验表明 Pollard 迭代函数与真正的随机函数相比运行效率要差一些 (相差一个大致为 1.2 的常数因子). 但是如果选择多个迭代函数，而且能够证明它的表现类似于随机游动，那么就可以得到期望的复杂度 [Teske, 1998].

Pollard 算法的空间复杂度取决于寻找匹配的过程. 最简单的方法是按第一个分量的次序储存 (x_i，a_i，b_i) (例如以均衡树的形式进行存储). 此时的存储量与 Shanks 方法一样都是 $O(\sqrt{n})$. 为此 Pollard 建议采用 Floyd 方法 (参见 [Knuth, 1997], Exercise 3.1.6) 来寻找匹配. 在该方法中不断计算 (x_i，a_i，b_i，x_{2i}，a_{2i}，b_{2i})，直至 $x_i = x_{2i}$. 显然当 $\lambda \mid i$ 且 $i \geqslant \mu$ 时，必有 $x_i = x_{2i}$，因此最终必定可以找到满足要求的 x_i，x_{2i}. 采用这样的方法以后，由于 x_{i+1}，$x_{2(i+1)}$ 可以通过迭代函数从 x_i，x_{2i} 中得到，即 $x_{i+1} = F(x_i)$，$x_{2(i+1)} = F(F(x_{2i}))$，因此并不需要多少存储空间. 由于 Floyd 方法并不一定能得到第一个匹配，因此 i 的期望值将比 λ 的期望值大；对于真正的随机映射来说，其期望值为

$$\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 1.03\sqrt{n}.$$

同时由于在得到序列 $\{x_i\}$，$\{x_{2i}\}$ 的过程中，$x_1, \cdots, x_i$ 被计算了两次，因此总的计算量平均为

$$3\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 3.09\sqrt{n}.$$

检测匹配更为有效的算法可参见 [Brent, 1980] 以及 [Schnorr and Lenstra 1984], Section 3.

ρ 算法可以通过并行计算来完成，即在不同机器上进行迭代操作，然后将得到的值传送到主服务器上，而主服务器的任务就是存储并检测匹配. 然而，如果计算得到的所有群元素都被储存，那么并行处理节省的时间将会被主服务器检测匹配的额外时间所抵消. 文献 [Oorschot and Wiener, 1999] 建议选取由易于识别的群元素构成的集合，例如所有二进制表示以连续的零开始的群元素. 在迭代过程中，只将得到的易于识别的元素传送至主服务器，然后再从新的起始值出发进行新的迭代过程. 如果该算法利用 M 台机器进行并行处理，那么其运行时间大致是串行 ρ 算法运行时间的 $1/M$.

4.3 Pohlig-Hellman 方法

如果群阶 n 不是一个素数，那么就可以利用 n 的素因子分解，把 G 中的离散对数问题转化为 G 的 Sylow 子群 中的离散对数问题. 进一步地，在 Sylow 子群中的离散对数问题可以进一步转化为对应的阶是素数的子群中的离散对数问题，其中 Sylow 子群是 G 中最大的素数阶子群，而且在这些子群中的离散对数可以归结为重复调用相对应的素数阶子群中的离散对数问题. 由此可知，当 p 是 n 的最大素因子时，文献 [Pohlig and Hellman, 1978] 中描述的下述算法的运行时间大致为 $O(\sqrt{p}\log p)$. 要注意该算法是由 Roland Silver, Richard Schroeppel 以及 H.Block 独立发现的.

设 n 的素因子分解为

$$n = \prod_{i=1}^{k} p_i^{v_i}.$$

如果所有的 p_i 都比较小，或者只是某一个 p_i 较大，则以上 n 的素因子分解是容易得到的. 如果 n 有若干个大素因子，那么此时 n 的素因子分解可能就是非常困难的. 但是既然 (大) 素数阶子群中的离散对数问题求解是困难的，因此实际上对该算法的应用并没有带来什么限制.

该算法的基本思想是通过确定 $l = \log_\alpha \beta \pmod{p_i^{v_i}}$, $i = 1, \cdots, k$ 并利用中国剩余定理来最终得到离散对数 $l = \log_\alpha \beta$.

为计算 $l \mod p^v$, 设 l 的 p 进制表示为

$$l \equiv \sum_{i=0}^{v-1} b_i p^i \mod p^v.$$

下面我们将递归地确定 b_i. 设 G_p 是 G 的 p 阶子群，$\gamma = \alpha^{\frac{n}{p}}$ 为其生成元，则

$$\beta^{\frac{n}{p}} = \alpha^{l\frac{n}{p}} = \gamma^l = \gamma^{b_0}.$$

因此 b_0 是 G_p 中 $\beta^{\frac{n}{p}}$ 关于 γ 的离散对数，即

$$b_0 = \log_\gamma \left(\beta^{\frac{n}{p}}\right),$$

因此其可以通过 4.1 节或 4.2 节中的方法得以确定. 设已知 $b_0, \cdots, b_{j-1}$，并令

$$l_j = \sum_{i=0}^{j-1} b_i p^i,$$

则有

$$(\beta\alpha^{-l_j})^{\frac{n}{p^{j+1}}} = \alpha^{(\sum_{i=j}^{v-1} b_i p^{i-j})\frac{n}{p}} = \gamma^{b_j},$$

所以 b_j 就是 G_p 中 $(\beta\alpha^{-l_j})^{\frac{n}{p^{j+1}}}$ 关于 γ 的离散对数，即

$$b_j = \log_\gamma\left((\beta\alpha^{-l_j})^{\frac{n}{p^{j+1}}}\right).$$

利用"平方－乘"算法 (即算法 1.1) 完成 $(\beta\alpha^{-l_j})^{\frac{n}{p^{j+1}}}$ 的计算需 $O(\log n)$ 次乘法，而求解 G_p 中的离散对数问题所需的计算量为 $O(\sqrt{p}\log p)$. 因此如果 p 是最大的素因子，$r = \sum_{i=1}^{k} v_i$ 是 n 素因子分解中素数的个数 (可能相同)，则对任意 $i = 1, \cdots, k$, 确定 $n \mod p_i^{v_i}$ 所需的计算量为

$$O\left(\sum_{i=1}^{k} v_i(\log n + \sqrt{p_i}\log p_i)\right) \subseteq O(r(\log n + \sqrt{p}\log p)).$$

对于 $n \mod p_i^{v_i}$，利用中国剩余定理得到最终的 n 需 $O(r\log^2 n)$ 次比特运算 (参见 [Cohen, 1993], pp.12–20). 由于要表示群元素至少需 $\log_2 n$ 个比特，从而任意的群运算至少需 $\log_2 n$ 次比特运算，因此算法最后一步对该算法总的计算复杂度并没有什么影响.

4.4 指标计算法

当 n 是一个大素数时，由于离散对数问题输入的大小为 $\Omega(\log n)$，因此前面提及的算法都是完全指数时间算法. 这一结果并不是偶然的：Shoup 在文献 [Shoup, 1997] 中指出适用于任意群中离散对数求解的算法都需 $\Omega(\sqrt{p}\log p)$ 个步骤，其中 p 是 n 的最大素因子. 由此在一般意义上，我们无法期望对 4.3 节中介绍的 Pohlig–Hellman 方法能够加以重大的改进. 换句话说，更高效的算法一定是针对某些特殊的具有特定结构的群而言的. 在本节中，将介绍适用于有限域乘法群的一个概率亚指数算法.

定义4.1 如果对于某个输入大小为 $\log n$ 的(非确定性)算法，存在常数 $c>0$, $\alpha \in [0,1)$，使得该算法运行时间的期望值为

$$L[\alpha,\ c] = O\left(\mathrm{e}^{(c+o(1))(\log n)^{\alpha}(\log\log n)^{1-\alpha}}\right),$$

则称该算法为亚指数算法 . 注意当 $\alpha = 0$ 时，该算法就是一个多项式算法，而当 $\alpha = 1$ 时，其就是完全指数时间算法.

指标计算法分以下两个步骤:

1. 线性方程组的获取.

固定由G 中元素组成的 因子基 $\Gamma=\{\gamma_1,\cdots,\gamma_t\}$. 我们的主要目的是确定每个 γ_i 的离散对数. 为此随机选取整数 $s\in\{0,\cdots,n-1\}$ 并计算 α^s. 如果 α^s 可以分解为因子基 Γ 中元素的乘积, 即

$$\alpha^s=\prod_{i=1}^{t}\gamma_i^{v_i},$$

则就可以得到 $\mathbb{Z}_n$ 中的线性方程

$$s=\sum_{i=1}^{t}v_i\log_\alpha\gamma_i.$$

如果获取了以上足够多的线性方程, 那么就可以求解得出每个 $\log_\alpha\gamma_i$, $i=1,\cdots,t$.

2. 离散对数的计算.

随机选取整数s, 并在 Γ 中尝试分解 $\beta\alpha^{-s}$. 如果分解成功, 即

$$\beta\alpha^{-s}=\prod_{i=1}^{t}\gamma_i^{v_i},$$

则

$$\log_\alpha\beta=s+\sum_{i=1}^{t}v_i\log_\alpha\gamma_i.$$

由于右式中的 s, v_i, $\log_\alpha\gamma_i$ 都是已知的, 因此就可以得出离散对数 $\log_\alpha\beta$.

由于因子基中元素的离散对数在计算 $\log_\alpha\beta$ 的过程中只使用一次, 因此需要在步骤 1 和步骤 2 所用的时间之间进行折中. 如果在步骤 1 中选取一个较大的因子基, 那么步骤 1 所需时间就会增加, 但同时会减少步骤 2 所需时间. 由此可见如果同一个域中需要计算的离散对数越多, 那么因子基也应当越大.

指标计算法的实用性取决于能否找到适当的因子基来构造相应的线性方程组. 到目前为止, 对于有限域、虚二次数域的类群 [McCurley, 1989] 以及大亏格超椭圆曲线的除子类群 (参见 [Adleman et al., 1994], [Müller et al. 1997], [Enge, 2001]), 已经找到了适当的因子基.

对于有限素域 $\mathbb{F}_p$, 很自然地取较小素数作为因子基中的元素, 并用 $\{0,\cdots,p{-}1\}$ 中的整数来表示群中的元素. 对于群元素 γ, 利用试除法在因子基中对 γ 加以分解, 即 γ 除以因子 γ_1 直至所得的商不再能被 γ_1 整除为止, 然后再对 γ_2 进行类似的处理, 以此类推. 若 $r\leqslant\log_2 p$ 是 γ 素因子分解中素数的个数 (可能相同), 则至多需

$t+r$ 次试除就可以在 Γ 中将 γ 分解，或者是证明 γ 在 Γ 中无法分解.

由于 $\mathbb{F}_{p^m}$ 中的元素都可以表示为 $\mathbb{F}_p[X]$ 中次数小于 m 的多项式，因此此时就可以以次数较小的不可约多项式作为因子基.

对于该算法有多种不同的改进策略. Blake, Fuji-Hara, Mullin 和 Vanstone 引入了所谓的 “系统方程 (systematic equations)”，使得步骤 1 中所需要的方程很大一部分可以很简单地获取 [Blake et al., 1984]. 利用 Coppersmith 有关多项式筛的算法，Gordon 和 McCurley 完成了 $\mathbb{F}_{2^{401}}$ 中离散对数问题的求解. 同时 Gordon 和 McCurley 认为 “$GF(2^{503})$ 中离散对数问题的求解可以在未来的 5 至 10 年内变成可能 ([Gordon and McCurley, 1993])”. 素域中的离散对数问题求解较为困难，目前的纪录是在十进制长度是 65 的素域中可以完成离散对数的求解 [Weber, 1996].

对于 $\mathbb{F}_p$, $\mathbb{F}_{2^m}$，Pomerance 提出的算法被严格证明其运行时间为 $L[1/2,\sqrt{2}]$(参见 [Pomerance, 1987]). 当 m,p 改变时，对于 $\mathbb{F}_{p^m}$ 上的离散对数问题目前还不知道是否存在亚指数算法. Lovorn Bender 证明了 $\mathbb{F}_{p^2}$ 上离散对数问题亚指数算法的存在性 (参见 [Bender, 1990]). 目前有一些算法被认为具有更快的运行时间，但这点并没有被严格证明. 在文献 [Gordom, 1993] 和 [Schirokauer, 1993] 对于 $\mathbb{F}_p$ 描述了基于数域筛法的指标计算法，其运行时间是 $L[1/3,4/\sqrt[3]{9}]$. 对于 $\mathbb{F}_{2^m}$，Coppersmith 提出的算法可以看成是数域筛法的特殊情况，其运行时间是 $L[1/3,c]$，其中 c 大致为 1.4(参见 [Coppersmith, 1984]). 这两种方法都可以用来得到前面提及的求解纪录. 与数域筛法类似地，文献 [Adleman, 1994] 提出了所谓的函数域筛法，对于 $\mathbb{F}_{2^m}$，其运行时间是 $L[1/3,\sqrt[3]{9}]$.

根据以上的结果，为确保安全性，一般要求基于有限域上离散对数问题的密码体制所采用的域的大小要 1000 比特左右.

要注意的是，步骤 1 中线性方程组的获取以及步骤 2 都容易进行并行处理. 实现过程中的瓶颈在于步骤 1 中获取的大量稀疏线性方程在 $\mathbb{Z}_n$ 中的求解. 更为高效的并行算法的提出将进一步推动指标计算法的应用.

4.5 椭圆曲线离散对数问题

椭圆曲线密码体制与基于有限域上离散对数问题的密码体制相比，突出的优势在于：除了少数几类曲线以外，到目前为止对于椭圆曲线上的离散对数问题没有亚指数算法.

指标计算法

Miller 指出对于椭圆曲线上的离散对数问题，与指标计算法类似的方法是不存

在的. 他的这一观点被 Silverman 和 Suzuki 从理论和计算实践上得到确认. 我们在这里给出其的一个大致描述, 建议有兴趣的读者进一步参阅文献 [Miller, 1986] 以及 [Silverman and Suzuki, 1998]. 设 E 是定义在有限素域 $\mathbb{F}_p$ 上的椭圆曲线, 则 E 的系数可以提升为整数. 我们考虑一种可能的提升 $E_{\mathbb{Q}}$. (对于定义在 $\mathbb{F}_{2^m}$ 上的椭圆曲线, 其系数可以提升为 m 次数域中的整数, 其中 2 不是惯性的. 此时的处理方式与 E 类似) 考虑 $E_{\mathbb{Z}_{(p)}}$, 其中

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

是 $\mathbb{Z}$ 在 p 处的局部环, 将 $E_{\mathbb{Z}_{(p)}}$ 上点的坐标进行模 p 约化, 就可以得到 $E_{\mathbb{F}_p}$ 上的点. 这样指标计算法就可以按以下方式进行: 确定由 $E_{\mathbb{F}_p}$ 上某些点构成的因子基, 并将其提升为 $E_{\mathbb{Z}_{(p)}}$ 中的点. 在 $E_{\mathbb{F}_p}$ 上随机选取元素并通过将其提升为 $E_{\mathbb{Z}_{(p)}}$ 中的点来进行 "分解", 从而可将其表示为提升后因子基中元素的线性组合. 这样约化后的点在 $E_{\mathbb{F}_p}$ 上也满足同样的线性关系.

不过目前并没有把 $E_{\mathbb{F}_p}$ 上的点提升到 $E_{\mathbb{Z}_{(p)}}$ 的简单方法, 而且只有当因子基中的点的高度比较小时, 整个算法才有效, 其中点 $\left(\frac{x}{d}, \frac{y}{d}\right)$, $x, y, d \in \mathbb{Z}$, $\gcd(x, y, d) = 1$ 的对数高度是指 $\log \max\{|x|, |y|, |d|\}$, 也就是在相差一个常数因子的意义下, 点的对数高度就是表示该点所需的十进制位数. 但是点 P 的倍点 nP 的对数高度增长是非常迅速的 (大致是 n^2 的关系). 在图 4.2 中, 纪录了有理曲线 $Y^2 = X^3 + X - 1$ 上点 $P = (1, 1)$ 各个倍点的 X 坐标 (从 $4P$ 开始). 图 4.2 是受文献 [Koblitz, 1998], p.143 中类似图表的启发而得到的.

另一方面, 由 Mordell-Weil 定理 (该定理可参见 [Husemöller, 1987], Chapter 6, [Lang, 1978], Chapter IV.2. [Silverman, 1986]) 知曲线 $E_{\mathbb{Q}}$ 上线性独立点的最大个数 (即其秩) 是有限的, 而且一般来说其秩是比较小的. 寻找秩较大曲线的方法来自于 Mestre. 其理论基础可参见 [Mestre, 1986], 而算法可参见 [Mestre, 1982]. 其基本思想是使曲线在模小素数所得的约化形式有尽可能多的点. 这就暗示了椭圆曲线诸系数在模所考虑的诸素数乘积时所需满足的条件. 尽管人们猜测存在秩为任意整数的椭圆曲线, 但目前纪录是存在一条椭圆曲线, 其秩被证明至少为 23(参见 [Martin and McMillen, 1997]).

由上可知, 很可能没有足够多的具有较小高度的点来构成一个适当的因子基. 因此对于一般椭圆曲线上的密码体制, 目前已知的攻击手段就是如同 4.1 节和 4.2 节所示的那样, 都是计算复杂度为 $O(\sqrt{n})$ 的算法. 但是对于某些特殊类型的曲线, 存在着特定的有效攻击方法.

$$\frac{25}{36}$$
$$\frac{685}{121}$$
$$\frac{7082}{2209}$$
$$\frac{154513}{196249}$$
$$\frac{9781441}{197136}$$
$$\frac{645430801}{468073225}$$
$$\frac{54088691834}{39890874529}$$
$$\frac{23545957758733}{430654875049}$$
$$\frac{2660536742331673}{3348618159624516}$$
$$\frac{3438505996705270765}{1099386223759472401}$$
$$\frac{238927973404332802853 0}{40848799798657292428 9}$$
$$\frac{2470536351695706691150273}{3568842156502352911081681}$$
$$\frac{91471740282015846956604 04993}{73825647682286700216286 2144}$$
$$\frac{404373028971550370031684692092 81}{198131190131379605085390118015 21}$$
$$\frac{142130019185439765346002547048069394}{144041052884595077187155035625188255}$$
$$\frac{40775514275390612683658186170700824879 81}{18432483027460656672609022221384024 1}$$
$$\frac{292477428367171815695731231266093809586286 33}{288544865462272835673815698728959220091462 44}$$
$$\frac{16446621836236050309439924597587179593680380899 33}{83901072785189703665402414145682292170060509588 1}$$
$$\frac{7679555980744445014603395204824802547437770648613257 0}{5623685827394653901724022330582419835420495478336929}$$
$$\frac{42072077105291274182838484613409656554635604853662899035 05}{60373907957065415403976427391323834292336484562142661050 01}$$
$$\frac{816297679393916005694837838808362431503501229559444925278681793}{148904572022531958307959435081656301977637384156037614895340176}$$
$$\frac{242513738949178952234806483689465816559631390124939658301320990605073}{737758370857134587907338874406776701992040735018075797266449328296 89}$$
$$\frac{37305812430327115580640557188334548355242580421878655283699578790767062474}{47803232530993255659471421491008524334965293857886857075847338386784976280}$$
$$\frac{67559659782039617237841184516992302782851604142385500859648938761010393239431661}{14936574510410904335660741815647139057367850205068241677325855756259592064080 25}$$

图 4.2 有理曲线 $Y^2 = X^3 + X - 1$ 上 $(1, 1)$ 的倍点

MOV 攻击

该攻击方法首先是由 Menezes, Okamoto 和 Vanstone 提出的. 该算法的基本思

想是将椭圆曲线离散对数问题约化为基域的某个扩域中的离散对数问题. 对于超奇异曲线来说, 通过这样的约化就可以得到亚指数算法. 在大体介绍文献 [Menezes et al., 1993a] 提出的方法之前, 我们用加法的语言重新叙述离散对数问题, 并考虑 $p \mid n$ 时的情况 (因为此时约化不能马上进行).

设 E 是定义在 $\mathbb{F}_q$ 上的椭圆曲线, $\operatorname{char}\mathbb{F}_q = p$, P 是 $E_{\mathbb{F}_q}$ 中阶等于 n 的点, $R = lP$, 其中 l 就是需要求解的离散对数. 和 Pohlig-Hellman 方法类似, 当 n 是合数, 例如 $n = n_1 n_2$ 时, 其中 $\gcd(n_1, n_2) = 1$, 只需分别确定 $l \mod n_1$, $l \mod n_2$ 即可, 然后就可以利用中国剩余定理得到最终的 l.

考虑 n_1 阶点 $n_2 P$ 以及点 $n_2 R$, 令

$$l_1 = \log_{n_2 P}(n_2 P).$$

由于 $n_2 R = l(n_2 P)$, 因此

$$l \equiv l_1 \pmod{n_1}.$$

同样地也可确定 $l \pmod{n_2}$.

设 $n = p^v n'$, $p \nmid n'$, 下面考虑在阶分别为 p^v, n' 的群中离散对数问题的求解. 当 p 较小时 (特别是当 $p = 2$ 时), p^v 阶群中的离散对数问题可以通过 Pohlig-Hellman 方法来完成. 因此不妨设 $\gcd(n, p) = 1$, 则由命题 3.37 知 $E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n$. MOV 约化算法如下所示:

1. 确定满足 $E[n] \subseteq E_{\mathbb{F}_{q^k}}$ 的最小整数 k.
2. 计算点 $Q \in E[n]$, 使得 $\alpha := e_n(P, Q)$ 是 n 阶本原单位根.
3. 计算 $\beta = e_n(R, Q)$, 其中 e_n 就是 3.7 节中描述的 Weil 对.
4. 在 $\mathbb{F}_{q^k}$ 中求解 $l = \log_P R = \log_\alpha \beta$.

由于

$$\beta = e_n(lP, Q) = e_n(P, Q)^l = \alpha^l$$

且 $\log_\alpha \beta$ 在模 n 的意义下是唯一确定的, 因此 MOV 算法必定成立. 要注意的是由引理 3.62 知满足要求的点 Q 是必定存在的. 同时利用 Miller 算法 (参见 [Menezes, 1993], pp. 63–68), Weil 对可以在概率多项式时间内完成计算.

对于超奇异曲线, 由定理 3.72 可知 $|E_{\mathbb{F}_q}| \equiv 1 \pmod{p}$, 因此 $p \nmid n$. 下面对于超奇异曲线, 我们仔细地研究如何完成 MOV 攻击中的步骤 1 和步骤 2. 表 4.1 列举了所需的信息, 其中常数 c 定义如下: 若 $E_{\mathbb{F}_q} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, n_1 \mid n_2$, 则 $E_{\mathbb{F}_{q^k}} \simeq \mathbb{Z}_{cn_2} \times \mathbb{Z}_{cn_2}$.

表 4.1 超奇异曲线上离散对数问题的约化

$t=q+1-\|E_{\mathbb{F}_q}\|$	群结构	n_2	k	c
0	循环群	$q+1$	2	1
0	$\mathbb{Z}_2\times\mathbb{Z}_{\frac{q+1}{2}}$	$\frac{q+1}{2}$	2	2
$\pm\sqrt{q}$	循环群	$q+1\mp\sqrt{q}$	3	$\sqrt{q}\pm 1$
$\pm\sqrt{2q}$	循环群	$q+1\mp\sqrt{2q}$	4	$q\pm\sqrt{2q}+1$
$\pm\sqrt{3q}$	循环群	$q+1\mp\sqrt{3q}$	6	$\frac{q+1}{q+1\pm\sqrt{3q}}$
$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1}\times\mathbb{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q}\mp 1$	1	1

利用 $E_{\mathbb{F}_{q^k}}$ 群指数 cn_2，就可以通过一个概率多项式时间算法来确定 Q，从而得到以下有效的约化算法：

1. 随机选取点 $Q'\in E_{\mathbb{F}_{q^k}}$，令 $Q=\frac{cn_2}{n}Q'$，并计算 $\alpha=e_n(P,Q)$.
2. 计算 $\beta=e_n(R,Q)$.
3. 在 $\mathbb{F}_{q^k}$ 中计算 $l'=\log_\alpha\beta$.
4. 若 $l'P=R$，则 $l=l'$；否则 α 不是 n 阶本原单位根，返回到步骤 2.

由此可见，建立在满足 $|t|=2\sqrt{q}$ 或 $t=0$ 的超奇异曲线上的 ElGamal 型密码体制并不比建立在基域或其二次扩域上的密码体制更为安全，因此并不值得为此进行额外的曲线上的群运算. 同时也应避免具有较小 k 值的非超奇异曲线. 有关 k 的一个易于检测的必要条件来自于下面的命题.

命题4.2 设 G 是一个有限交换群，

$$G\simeq\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2},\quad n_1,n_2\geqslant 1,\quad n_1\mid n_2,$$

H 是 G 的一个子群，则

$$H\simeq\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2},$$

其中 m_1，$m_2\geqslant 1$，$m_1\mid m_2$ 且 $m_1\mid n_1$，$m_2\mid n_2$.

注意 由命题 4.2 可知，如果 G 是至多两个循环子群 G_i 的内积，且 $|G_1|$ 整除 $|G_2|$，则 H 也至多是相同个数的循环子群 H_i 的内积，且 $|H_i|\mid|G_i|$. 但是这并不意味着 H_i 一定是 G_i 的子群. 一个简单的反例是：令 $H=\langle(1,1)\rangle$ 是 $\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}$ 由 $(1,1)$ 生成的子群 (直观上看，该子群是沿着对角线方向倾斜在该群中). 如果 $n_1>1$，则有 $m_1=1,m_2=n_2$，满足命题中的条件，但是 $H\not\subseteq\mathbb{Z}_{n_2}$.

证明　实际上对于拥有两个以上生成元的交换群，命题 4.2 仍然成立 (参见 [Hall, 1959], Theorem 3.3.3). 由于大多数代数书并没有介绍该命题，我们在这里对命题中给定的特殊情况给出一个初等的证明. 记 $G[n]$ 表示 G 中所有 n 阶扭元素构成的集合，而

$$G[n^\infty] := \bigcup_{i=0}^{\infty} G[n^i]$$

表示 G 中所有阶整除 n 的幂次的元素构成的集合. 对于 $|G|$ 的某个素因子 p，子群 $G[p^\infty]$ 就是 G 的 p-Sylow 子群，即阶为 p 的幂次的最大子群. 由引理 3.49 可得

$$G \simeq \mathop{\times}_{p||G|} G[p^\infty] \simeq \mathop{\times}_{p||G|} (\mathbb{Z}_{p^{v_1}} \times \mathbb{Z}_{p^{v_2}}),$$

其中 v_i 满足 $p^{v_i} \mid n_i$，$p^{v_i+1} \nmid n_i$. 由此可知只要对 p-Sylow 子群证明该命题，然后利用中国剩余定理即可完成整个命题的证明. 设

$$G \simeq \mathbb{Z}_{p^{v_1}} \times \mathbb{Z}_{p^{v_2}}, \quad 0 \leqslant v_1 \leqslant v_2,$$

如果 G 是一个循环群，即 $v_1 = 0$ 时，则由于循环群的任意一个子群也是循环群及 $|H| \mid |G|$，可知命题成立. 否则由交换群基本定理 3.47 以及 $|H| \mid |G|$ 可知

$$H \simeq \mathbb{Z}_{p^{\mu_1}} \times \cdots \mathbb{Z}_{p^{\mu_s}}, \quad 1 \leqslant \mu_1 \leqslant \cdots \leqslant \mu_s.$$

首先说明 $s \leqslant 2$. 由于

$$G[p] \simeq p^{v_1-1}\mathbb{Z}_{p^{v_1}} \times p^{v_2-1}\mathbb{Z}_{p^{v_2}} \simeq \mathbb{Z}_p \times \mathbb{Z}_p,$$

因此 $|G[p]| = p^2$. 同样地有 $|H[p]| = p^s$. 由于 $H[p] \subseteq G[p]$，因此 $s \leqslant 2$.

通过令 $\mu_1 = 0$，我们总可以设 $s = 2$，则显然有 $\mu_2 \leqslant v_2$. 若 $\mu_1 > v_1$，则有 $v_2 \geqslant \mu_2 \geqslant \mu_1 > v_1$，从而

$$|G[p^{\mu_1}]| = p^{v_1}p^{\mu_1} < p^{\mu_1}p^{\mu_1} = |H[p^{\mu_1}]|.$$

矛盾.　□

为得到关于 k 的必要条件，首先由定理 3.76 可知 $E_{\mathbb{F}_{q^k}} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$，其中 $n_1 \mid q^k - 1$. 由于 $E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n$ 是 $E_{\mathbb{F}_{q^k}}$ 的子群，因此由命题 4.2 可知 $n|n_1, n|q^k - 1$.

利用 Tate 对而不是 Weil 对的类似约化算法可参见 [Frey and Rück, 1994]. 该约化能够应用到扩域 $\mathbb{F}_{q^k}$ 的乘法群的充要条件是 $n \mid q^k - 1$.

由上可知，在利用定义在 $\mathbb{F}_q$ 上的曲线来设计椭圆曲线密码体制并将安全性建立在 n 阶子群中离散对数问题的难解性时，必须确保 $\mathbb{F}_{q^k}^\times$ 中求解离散对数问题是计算不可行的，其中 k 是满足 $n|q^k - 1$ 的最小整数.

迹为 1 的曲线

虽然 MOV 约化特别适用于攻击超奇异曲线. 由 Waterhouse 定理 3.72 知, 超奇异椭圆曲线的阶模 p 同余 1. 但是对于下列的一类椭圆曲线, 它们的阶是域特征 p 的倍数, 存在着更为有效的攻击方法. 该攻击方法在文献 [Satoh and Araki, 1999] [Semaev, 1998]和 [Smart, 1999] 中被独立地提出.

设 $n = p^v n'$, $p \nmid n'$, 则只需计算 $l \equiv \log_P R \pmod{p^v}$ 以及 $l \equiv \log_P R \pmod{n'}$ 即可. 为计算 $l \mod p^v$, 只需利用 4.3 节中介绍的 Pohilg–Hellman 方法, 在由 $\frac{n}{p}P$ 生成的 p 阶子群中完成 v 个离散对数的求解即可. 而为完成 p 阶子群中离散对数问题的求解, 新算法是通过将其约化为加法群 $\mathbb{F}_p = \{0, \cdots, p-1\}$ 中的离散对数问题, 使得在多项式时间内完成问题的求解. 注意只有当 p 较大时, 这样做才是有意义的 (当 p 较小时, p 阶子群中的离散对数总是容易求解的). 特别地, 当曲线是定义在素域 $\mathbb{F}_p$ 上时, 由 Hasse 定理 3.61 知 $n|p$ 等价于 $n = p$, 也就是 Frobenius 自同态的迹等于 1.

文献 [Semaev, 1998] 中对该方法的描述是比较初等的, 而利用第 3 章中介绍的相关知识完全就可以理解.

Xedni 计算

Silverman 提出了一个算法, 该算法在下面的意义下是指标计算法的逆过程: 首先将一些点提升到 $\mathbb{Q}$ 中, 然后再选取曲线, 使得提升后的曲线通过这些点 (可参阅 [Silverman, 2000]). 由于此时提升过程是非常简单的, 因此这样处理就克服了在介绍椭圆曲线指标计算法时所提及的提升问题. 其基本思想是将提升后点在 $\mathbb{Z}$ 上的线性关系转化为原始曲线上点的线性关系, 以此来确定离散对数. 不幸的是, 提升后的点很可能是线性无关的. 为此 Silverman 建议使用反向 Mestre 条件, 即选取某条有理曲线, 使其模小素数后得到的约化形式有尽可能少的点. 这样处理就很可能增加曲线具有较小秩的可能性. Koblitz 指出有效的 xedni 计算可以被用于求解有限素域中的离散对数问题以及整数分解问题, 从而危及目前使用的所有公钥密码的安全性 [Silverman, 2000], Appendix A. 以加拿大滑铁卢大学为中心的研究小组目前正在研究该算法的实用性 [Jacobson et al., 2000].

Certicom 公司的 ECC 挑战

加拿大 Certicom 公司受 RSA 关于大整数分解挑战的启发, 提出 ECC 挑战. 该挑战的任务是完成以素域或特征为 2 的有限域为基域的随机椭圆曲线或 Koblitz曲线(其定义在 $\mathbb{F}_2$ 上, 而点的坐标属于某个扩域 $\mathbb{F}_{2^m}$) 上离散对数问题的求解 [Certi-

com, 1997]. 到目前为止，利用并行 Pollard ρ 算法已经完成了对定义在元素个数略小于 2^{100} 的有限域上的椭圆曲线离散对数问题的攻击 (参见 [Escott, 1998] 和 [Certicom, 1997]). 文献 [Gallant et al., 2000] 和 [Wiener and Zuccherato, 1998] 指出利用 Koblitz 曲线的特殊结构可以进一步提高 ρ 算法的运行速度，与 $\mathbb{F}_{2^m}$ 上的随机曲线相比可以大致提高 $\sqrt{m}$ 倍. 改进后的算法使用了 Frobenius 自同态 $(x, y) \mapsto (x^2, y^2)$.

第 5 章　椭圆曲线上点数的计算

我们在第 4 章中已经看到，对于一个基于离散对数问题的密码体制，其安全性主要取决于所使用的群的阶，除非是特殊的结构使得可以用更为有效的方法来攻破该体制. 如果群阶充分大，那么诸如 Shanks 的大步–小步法或者 Pollard 的 ρ 算法等平方根攻击方法都是无效的. 我们可以采用下面两种方法来避免 Pohlig-Hellman 攻击.

第一种做法是选择阶未知的群，这样 Pohlig-Hellman 方法就不起作用. 但是这种做法有一定的风险，因为还没有哪一类已知类型的群，计算该群阶存在理论上的障碍. 由于目前我们还不知道对于任意的群，求其群阶是否为 NP 完全问题，因此有可能出现如下的情况：当选择一个群时，攻击者可能恰好拥有计算该群阶的某个算法. 另外，上述做法只适用于加密信息，而第 1 章所介绍的签名算法就需要知道所使用的群的阶.

抵抗 Pohlig-Hellman 攻击的第二种行之有效的做法就是选取群阶中有大的素因子的群. 对于椭圆曲线的情形，可有很多种方法. 首先，可以利用复乘算法构造出具有合适阶的椭圆曲线 ([Atkin and Morain, 1993] 和 [Lay and Zimmer, 1994]). 其次，可以选择一些容易计算阶的特殊类型的曲线，例如超奇异椭圆曲线 (参阅定理 3.72)，或者定义在小域上的曲线，但在扩域中考虑曲线的点群 (参阅定理 3.66). 由于根据前面 4.5 节的讨论知，超奇异椭圆曲线是不建议使用的，到目前为止，还没有找到对定义在子域上椭圆曲线有效的攻击办法. 然而，存在一类特殊的曲线和一种普遍承认的选择椭圆曲线的最安全做法，这就是先固定一个基域，然后随机选择曲线，即选取定义参数，再计算点群的阶，直至找到阶具有大素因子的曲线. 由于最近十几年来算法方面的进展，上面的做法已经变得切实可行.

在这一章中，我们总假定 $k = \mathbb{F}_q = \mathbb{F}_{p^m}$ 是一个特征为 p 的有限域，而 E 是定义在 k 上的椭圆曲线.

5.1　大步–小步算法

在第 4.1 节中，我们介绍了用大步–小步的方法计算任意的群中元素 β 关于基 α 的离散对数，也就是计算出满足 $\alpha^k = \beta$ 的最小正整数 k. 从本质上说，这个算

法可以计算元素 α 的阶，即满足 $\alpha^k = 1$ 的最小正整数 k. 如果 E_k 是循环群，而且已知它的生成元，则可以利用这种算法计算 E_k 的阶. 为确定 E_k 的生成元，可以通过检测一个随机元素，直至找到生成元的方法来得到解决. 对于前者，由 3.12 节可知 E_k 是由两个元素生成，我们可以随机选择两个生成元，计算它们生成子群的阶，从而得到 E_k 的阶. 进一步地，对于密码应用而言，只要在 E_k 上取一个点，然后检查它的阶是否有一个大素因子就可以了. 但是无论哪种情况，我们都需要知道如何在 E_k 上取一个随机点.

算法5.1 (在 E_k 上随机取点) *下面概率型算法能够 (几乎) 均匀一致地产生 E_k 上的随机点. 对于 $p \neq 2$ 的情形，需要域 k 中运算次数的期望为 $O(\log q)$，对于 $p = 2$ 的情形，期望为 $O(\log^2 q)$.*

1. *随机选取 $x \in k$，这一步可以均匀一致地进行.*
2. *在 k 中求解方程 $E(x, Y) = 0$. 如果在 k 中存在一个解 y，则 $-y - a_1x - a_3$ 就是第二个解. 在两者之间随机选取一个，就得到 E_k 上的一个点 $P = (x, y)$. 否则返回 1.*

算法 5.1 得到的点的分布不完全是均匀一致的，因为选择 2 阶点的概率是选择其他点的两倍，而无穷远点 $\mathcal{O}$ 永远不可能被选取. 第一个问题可以通过预先计算 2 阶点的 X 坐标，然后在第 1 步中以选取其他值概率的 1/2 来选取这些 X 值. 第二个问题实际上并不重要，因为在后面的算法中我们只对有限点感兴趣. 不管怎样，除至多 4 个点以外，我们选取点的方式是均匀一致的.

证明 对于任意给定的常数 $c < 1/2$ 及充分大的 q，每一轮算法的成功概率为

$$
\begin{aligned}
&\frac{E_k \text{ 中所有有限点的不同 } X \text{ 坐标的个数}}{q} \\
\geqslant &\frac{(|E_k| - 1)/2}{q} \\
\geqslant &\frac{q - 2\sqrt{q}}{2q} \qquad \text{(Hasse 定理)} \\
= &\frac{1}{2} - \frac{1}{\sqrt{q}} \\
\geqslant &c.
\end{aligned}
$$

因此算法运行轮数的期望是 $O(1)$.

剩下的问题就是估计每一轮的运行时间，即在 k 中求解二次方程 $f = Y^2+$

$aY+b$ 所需时间的期望值. 由命题 3.67 可知，判断一个二次方程是否有解是简单的. 假设 f 在 k 中有解，则当 $p\neq 2$ 时，能够利用 Berlekamp-Rabin 算法求解，其运算次数的期望是 $O(\log q)$(算法的具体细节可参阅 [Menezes et al., 1993a], pp.22–23). 如果 $p=2$ 且 $a=0$，则 f 的二重根是 $b^{2^{m-1}}$. 当 $a\neq 0$ 时，f 的根是不同的，并且可以利用确定性的 Berlekamp 迹算法在 $O(\log^2 q)$ 次运算下完成求解过程 (可参阅 [Menezes et al., 1993a], pp.23–24). □

先不考虑 E_k 可能不是循环群的情况，而把注意力集中到计算单个点的阶. 如果知道某些额外的信息，那么就可以很简单地计算点的阶.

算法5.2 (计算 n 扭点的阶) 假设 G 是加法群，$\mathcal{O}$ 是单位元，$P\in G$ 是一个 n 扭点，并且 n 的素因子分解是已知的. 那么下面的算法可在 $O(\log^2 n)$ 次群运算内计算出 P 的阶：

对于 n 的每一个素因子 l，只要 $\dfrac{n}{l}P=\mathcal{O}$，就用 $\dfrac{n}{l}$ 代替 n.

证明 显然上面的算法能够计算出 P 的阶. 如果

$$n=\prod_{i=1}^{r} l_i^{v_i}$$

是 n 的素因子分解，那么最多需要 $\sum\limits_{i=1}^{r} v_i$ 次关于 P 的倍数运算，利用逐次平方算法 1.1，每一次 P 的倍数运算需要 $O(\log n)$ 次群运算. 由于 $s\leqslant \log_2 n$，因此算法中关于计算复杂度的结论成立. □

如果预先知道的信息很少，那么当我们知道 P 点阶的某个上界时，就可以使用大步-小步的方法计算点的阶. 下面的是一个更一般的算法，该算法在后面计算 E_k 中的点数时将被用做一个子程序.

算法5.3 (任意点的阶) 设 G 是群且 $P\in G$，$1\leqslant C<B$，$1\leqslant L$ 和 $0\leqslant l_1<L$ 都是整数. 下面的算法能够计算出满足条件 $l\in[C,B]$ 的最小整数 l(如果这样的整数存在的话)，使得 $lP=\mathcal{O}$ 且 $l\equiv l_1 \pmod L$. 进一步地，如果 LP 的阶不超过 $(B-C+2)/L-2$，则输出的也恰好是 LP 的阶. 该算法需要 $O\big(\sqrt{(B-C)/L}\big)$ 次群运算，还需要存储 $O\big(\sqrt{(B-C)/L}\big)$ 个群元素.

1. 设

$$C_1=\min\{c\in[C,B]: c\equiv l_1 \pmod L\},$$
$$B_1=\max\{c\in[C,B]: c\equiv l_1 \pmod L\}.$$

(a) 如果 C_1 和 B_1 不存在，则停止.

(b) 如果 $C_1 = B_1$ 且 $C_1P = \mathcal{O}$, 则输出 $l = C_1$ 并停止.

(c) 如果 $C_1 = B_1$ 且 $C_1P \neq \mathrm{O}$, 则停止.

(d) 否则计算 $P_1 = LP$, $s = \left\lceil \sqrt{(B_1 - C_1)/L + 1} \right\rceil$ 和 sP_1.

2. 对于每一个 i, $0 \leqslant i < s$, 计算 (iP_1, i), 并按照第一个分量进行排序存储.
3. 对于所有的 j, $0 \leqslant j < s$, 递归地计算

$$-C_1P - jsP_1 = (-C_1P - (j-1)sP_1) - sP_1.$$

然后在第 2 步得到的预计算表中查找该群元素, 所得结果是按字典序排列的匹配对 (j, i). 把满足 $C_1 + (js + i)L > B_1$ 的匹配对 (j, i) 舍弃.

4. 如果没有找到匹配对, 则停止. 否则以 $l = C_1 + (js + i)L$ 的形式输出第一个匹配对 (j, i). 如果找到两个相继的匹配对 (j_1, i_1) 和 (j_2, i_2), 则 LP 的阶就是 $(j_2 - j_1)s + (i_2 - i_1)$.

证明 关于该算法的正确性. 首先注意到我们所需的实际上是下面集合的最小元素:

$$\begin{aligned} &\{l \in [C, B] \,|\, lP = \mathcal{O}, \quad l \equiv l_1 \pmod L\} \\ =&\left\{C_1 + kL : k \in \left[0, \frac{B_1 - C_1}{L}\right], \quad (C_1 + kL)P = C_1P + kP_1 = \mathcal{O}\right\}. \end{aligned}$$

而一个匹配 (j, i) 意味着

$$-C_1P - jsP_1 = iP_1,$$

这等价于

$$C_1P + (js + i)P_1 = \mathcal{O}.$$

由于区间 $[0, (B_1 - C_1)/L]$ 中的每一个元素都可以表示成 $js + i$ 的形式, 而且 $0 \leqslant i, j < s$, 从而可以确保不会遗漏其他的匹配.

很显然, 如果我们能够找到两个匹配, 则该算法能够正确地计算出 P_1 的阶. 只有当 P_1 的阶 $\operatorname{ord} P_1 \leqslant (B_1 - C_1)/L$ 时, 上述情况才能发生. 由

$$C_1 \leqslant C + (L-1), \quad B_1 \geqslant B - (L-1)$$

可知

$$(B_1 - C_1)/L \geqslant (B - C + 2)/L - 2.$$

因此只要输出的值不超过 $(B - C + 2)/L - 2$, 则输出的必定是 P_1 的阶 $\operatorname{ord} P_1$.

该算法的时间、空间复杂度可以和 4.1 节类似地加以证明. □

为处理有两个生成元 P 和 P' 的情况，我们需要计算 P' 在商群 $E_k/\langle P\rangle$ 中的阶. 此时仍然可以采用大步-小步法.

算法5.4 (点在商群中的阶) 设 G 是群，$H=\langle P\rangle$ 是 G 的一个正规的循环子群，P' 是 G 中的另外一个点. 假设已知 $l=\mathrm{ord}_G P$，$l'=\mathrm{ord}_G P'$. 下面的算法能够在 $O\left(\sqrt{\tilde{l}}\log^2\tilde{l}\right)$ 次群运算时间内计算出 P' 在商群 G/H 中的阶 $\mathrm{ord}_{G/H}P'$，该算法所需要存储的群元素个数为 $O\left(\sqrt{\tilde{l}}\right)$，其中 $\tilde{l}=\max\{l,l'\}$.

1. 令 $h=l'$, $s=\left\lceil\sqrt{\tilde{l}}\right\rceil$，并利用诸如试除等方法分解 l'.
2. 计算 $\mathcal{B}=\{iP:0\leqslant i<s\}$ 并按照通常的方式存储起来. 设 $\mathcal{G}=\{jsP:0\leqslant j<s\}$.
3. 对于 l' 的每一个素因子 p'，利用下面的第4步测试是否有 $(h/p')P'\in\langle P\rangle$. 如果 $(h/p')P'\in\langle P\rangle$，则用 h/p' 代替 h 重复进行测试. 否则处理 l' 的下一个素因子. 最后得到的 h 就是所求的阶.
4. 对于任意的 $Q\in\mathcal{G}$，在 $\mathcal{B}$ 中查找 $(h/p')P'-Q$. 如果查找成功，则 $(h/p')P'\in\langle P\rangle$，否则 $(h/p')P'\notin\langle P\rangle$.

证明 该算法实际上是算法 5.2, 5.3 的结合. 我们知道 $l'P'=\mathcal{O}$，从而 $l'P'\in\langle P\rangle$. 所以要证明该算法的正确性，只要说明第 4 步的正确性即可. 由 $\mathcal{B}$ 和 $\mathcal{G}$ 的构造可知

$$\begin{aligned}\mathcal{B}+\mathcal{G}&=\{(i+js)P:0\leqslant i,\quad j<s\}\\&=\left\{iP:0\leqslant i<\left\lceil\sqrt{\tilde{l}}\right\rceil^2\right\}\\&=\langle P\rangle,\end{aligned}$$

而且在第 4 步中出现匹配等价于 $(h/p')P'\in\mathcal{B}+\mathcal{G}\in\langle P\rangle$，从而算法是正确的.

下面考虑时间复杂度. 运行一次第 4 步需要用 $O(\log l')$ 次乘法来计算 $(h/p')P$，需要 $O(\sqrt{\tilde{l}}\log\tilde{l})$ 次群运算来完成减法，还需要一个查找过程. 这样的步骤至多被调用 $\log_2 l'$ 次. 利用试除法分解 l' 需要 $O(\sqrt{l'})$ 次除法，而每次除法所需计算量至多相当于一次群的求逆运算. 最后对 $\mathcal{B}$ 进行计算和排序需 $O(\sqrt{\tilde{l}}\log\tilde{l})$ 次运算，从而总的计算复杂度是

$$O\left(\log^2 l'+\sqrt{\tilde{l}}\log\tilde{l}\log l'+\sqrt{l'}\right)\subseteq O\left(\sqrt{\tilde{l}}\log^2\tilde{l}\right).$$

和前面算法一样，可以得到算法中对空间复杂度的估计. □

有了上面的子程序，我们就可以很容易给出计算 $|E_i|$ 的算法如下.

算法5.5 (E_k 的阶)　设 E 是定义在有限域 $k=\mathbb{F}_q$ 上的椭圆曲线. 下面的概率型算法能够计算出 $|E_k|$, 该算法所需要群运算次数的期望 $O(\sqrt[4]{q}\log^2 q\log\log q)$, 需存储的群元素个数为 $O(\sqrt[4]{q})$.

1. 利用算法5.1随机选择点 $P\in E_k\setminus\{\mathcal{O}\}$. 以 $C=q+1-\lfloor 2\sqrt{q}\rfloor$, $B=q+1+\lfloor 2\sqrt{q}\rfloor$, $L=1$, $l_1=0$ 作为输入参数调用算法5.3. 如果只找到一个 $r\in[C,B]$ 满足 $rP=\mathcal{O}$, 则 $|E_k|=r$; 否则我们计算出阶 $l=\mathrm{ord}_G P$.
2. 随机选择第二个点 $P'\in E_k\setminus\{\mathcal{O}\}$, 并以 $L=l$, $l_1=0$ 为输入参数再次调用算法5.3. 如果找到唯一的 $r'\in[C,B]$ 满足 $r'P'=\mathcal{O}$, 则 $|E_k|=r'$; 否则我们计算出阶 $L'=\mathrm{ord}_G lP'$. 这时由于 P' 的阶 l' 是 lL' 的因子, 因此可调用算法5.2计算出阶 $l'=\mathrm{ord}_G P'$. 必要的时候可以交换 P 和 P', 以保证 $l\geqslant l'$.
3. 利用算法5.4计算 P' 在商群中的阶 $t=\mathrm{ord}_{E_k/\langle P\rangle}P'$. 如果 $lt>2\lfloor 2\sqrt{q}\rfloor$, 则 $|E_k|$ 是 $[C,B]$ 中唯一能够被 lt 整除的数; 否则返回到第2步.

证明　首先说明如果该算法能够中止, 则必定输出正确的结果. 由 Hasse 定理知 $|E_k|\in[C,B]$, 而且在固定了点 P 之后, 有 $l=\mathrm{ord}_G P$ 是 $|E_k|$ 的因子. 在第 1 步中我们判断是否只有一个可能的候选值满足要求, 因此如果算法在第 1 步时中止, 则只有一个匹配值, 也就是说 P 点的阶 $l>2\lfloor 2\sqrt{q}\rfloor$, 因而输出的结果也是正确的. 否则就有 $l\leqslant 2\lfloor 2\sqrt{q}\rfloor$. 在第 2 步中, 我们取第二个点 P', 并测试在 Hasse 区间 $[C,B]$ 中是否存在多个 l 和 l' 的公倍数. 由于 $|E_k|$ 一定是 l 和 l' 的的公倍数, 因此如果在此区间中只有一个公倍数, 则它就是 $|E_k|$. 最后在第 3 步中我们计算

$$lt=\mathrm{ord}_{E_k}P\cdot\mathrm{ord}_{E_k/\langle P\rangle}P'=|\langle P,P'\rangle|,$$

它必定整除 $|E_k|$.

注意到当该算法所使用的点对 (P,P') 恰好是 E_k 的生成元时, 算法就会中止, 因此算法中止的概率大于 0.

由算法 5.2 到算法 5.4 的复杂度分析可知, 该算法运行一轮所需时间是 $O(\sqrt[4]{q}\log^2 q)$. 而算法 5.2 中分解 lL' 需 $O(\sqrt{lL'})\subseteq O(\sqrt[4]{q})$ 次试除. 由于存在多种多样可能的终止条件, 计算该算法运行轮数的期望值是困难的. 为简化讨论, 我们对该算法进行细微的改变, 即在第 3 步中把 "返回第 2 步" 变为 "返回第 1 步". 我们从每一轮成功概率的下界出发, 推导出运行轮数期望值的上界. 设 $E_k\simeq\mathbb{Z}_m\times\mathbb{Z}_n$, 其中 $m|n$, 如果在某一轮中 $l=n$, $t>(2\lfloor 2\sqrt{q}\rfloor)/n$, 则该轮一定成功. 下面我们考虑选取满足这些条件的随机点对 (P,P') 的概率.

1. 如果 $n>2\lfloor 2\sqrt{q}\rfloor$. 则任一满足条件 $l=n$ 的点对就会导致算法成功. 在 $mn-1$ 个可能选取的 P 中有 $m\varphi(n)$ 个点的阶是 n, 因此该轮成功概率至少是 $\varphi(n)/n$.

2. 如果 $n \leqslant 2\lfloor 2\sqrt{q} \rfloor$. 由

$$|E_k| = mn \geqslant q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2$$

可知 $n \geqslant \sqrt{q} - 1$. 因此对于较大的 q，当点对满足 $l = n, t \geqslant 5$ 时一定成功，具体地说就是

$$5(\sqrt{q} - 1) > 2\lceil 2\sqrt{q} \rceil \iff q \geqslant 25.$$

选取合适 P 的概率是 $\varphi(n)/n$，当 $t < 5$ 时 P' 的数目为

$$\begin{aligned}
|\{P' \in E_k : t < 5\}| &= |\{P' \in E_k : 3P' \in \langle P \rangle \text{ 或} 4P' \in \langle P \rangle\}| \\
&\leqslant |[3]^{-1}(\langle P \rangle)| + |[4]^{-1}(\langle P \rangle)| \\
&= |\langle P \rangle|\big(|E[3]| + |E[4]|\big) \\
&\geqslant n(9 + 16) \qquad\qquad (\text{定理3.39}) \\
&= 25n.
\end{aligned}$$

因此合适的点 P' 所占的比例至少是

$$\frac{mn - 25n}{mn - 1} \geqslant \frac{(m - 25)n}{mn} = 1 - \frac{25}{m}.$$

注意到

$$q - 2\sqrt{q} < mn \leqslant 4\sqrt{q}m$$

意味着

$$m > \frac{1}{4}\sqrt{q} - \frac{1}{2} \to \infty \qquad (q \to \infty),$$

所以对于任一正常数 ε 以及充分大的 q，合适的点 P' 所占的比例至少是 $1 - \varepsilon$.

因此，在这种情况下选取能够成功的点对 (P, P') 的概率还接近于 $\varphi(n)/n$. 因此，在算法成功之前所需要运行轮数的期望至多是

$$\begin{aligned}
\sum_{i=1}^{\infty} i\left(1 - \frac{\varphi(n)}{n}\right)^{i-1} \frac{\varphi(n)}{n} &= \frac{\varphi(n)}{n}\left(\frac{\partial}{\partial c}\frac{1}{1-c}\right)\bigg|_{c=1-\frac{\varphi(n)}{n}} \\
&= \frac{\varphi(n)}{n}\frac{1}{(1-c)^2}\bigg|_{1-c=\frac{\varphi(n)}{n}} \\
&= \frac{n}{\varphi(n)}.
\end{aligned}$$

剩下的是用 q 的形式给出 $n/\varphi(n)$ 的一个上界，这是一个不平凡的结论，因为

$$\frac{n}{\varphi(n)} = \prod_{r|n,\, r\text{素}} \frac{1}{1 - \frac{1}{r}}$$

不仅仅与 n 的大小有关，还与 n 的素因子有关. 由 [Rosser and Schoenfeld, 1962] 中第 72 页的结论

$$\frac{n}{\varphi(n)} < e^C \log\log n + \frac{3}{\log\log n},$$

其中 $C = 0.5772\cdots$ 是欧拉常数，因此有

$$\frac{n}{\varphi(n)} \in O(\log\log q).$$

从而对任意的 $\varepsilon > 0$，算法的运行时间复杂度的期望值是

$$O\left(\sqrt[4]{q}\log^2 q \log\log q\right) \subseteq O\left(\sqrt[4]{q}\log^3 q\right) \subseteq O\left(q^{\frac{1}{4}+\varepsilon}\right). \qquad \square$$

注　可以证明，在第二种情况下，能够生成整个群的随机点对 (P, P') 出现的概率至少是

$$\begin{aligned}\frac{\varphi(m)\varphi(n)}{mn} &\geqslant \left(e^C \log\log n + \frac{3}{\log\log n}\right)^{-2} \\ &\geqslant \left(e^C \log\log(4\sqrt{q}) + \frac{3}{\log\log(4\sqrt{q})}\right)^{-2}.\end{aligned}$$

当 $q \approx 10^{25}$ 时，该值大约是 2.1%. 因此算法平均不超过 50 轮，就可以得到一个生成点对. 对于满足第一种情况的椭圆曲线循环点群，平均只要 8 轮即可.

利用类似的方法，Müller 成功地计算出 $|E_k|$，他选择的素域 k 的大小大致是 10^{25}(参见 [Müller, 1991], p.103). 他发现在所考虑的曲线中，大约有 80% 是循环的 [Müller, 1991], pp.107–109，从而只需重复第 1 步就可以计算出椭圆曲线的群阶.

5.2　Schoof 算法

在计算椭圆曲线有限群阶的问题上，Schoof([Schoof, 1985]) 首先取得理论上的突破. 他利用 Hasse 定理，提出计算椭圆曲线有限群阶的确定型多项式时间算法.

回忆以前的记号：令 t 表示 $(q+1) - |E_k|$，$\varphi:\ (x,y) \mapsto (x^q, y^q)$ 表示 Frobenius 自同态，则由定理 3.61 可知 t 是满足

$$\varphi^2 - t\varphi + q = 0; \tag{5.1}$$

的唯一整数，且有不等式

$$|t| \leqslant 2\sqrt{q}.$$

由上面的不等式可知，要确定椭圆曲线有限群阶 $|E_k|$，只需计算 $t \pmod L$ 即可，其中 L 是大于 $4\sqrt{q}$ 的任意整数. 因此问题可以简化如下：对于不等于 2 和 p 的素

数 l, 计算 $t \pmod{l}$. 当这样的素数之积大于 $4\sqrt{q}$ 时，利用中国剩余定理就可以计算出 t 的准确值.

为了计算 $t \pmod{l}$, 将 (5.1) 式限制到 l 扭点 $E[l]$ 上可得

$$\varphi_l^2 - t\varphi_l + q = 0, \tag{5.2}$$

其中 φ_l 是 φ 在 $E[l]$ 上的限制. 于是 (5.2) 可看作 $\mathbb{Z}_l$ 代数 $\mathrm{End}(E)|_{E[l]}$ 中的恒等式 (可参阅 Hasse 定理 3.61 的证明).

记 s 为 q 模 l 的最小正余数，则对任意的 τ, $0 \leqslant \tau < l$, 我们需要验证等式

$$\varphi_l^2 + s = \tau\varphi_l \tag{5.3}$$

是否成立. 如果 τ_0 是一个解，则 $t \equiv \tau_0 \pmod{l}$.

为了判断某一个由多项式或有理函数构成的关系式在 $E[l]$ 上是否成立，我们需要利用除子多项式 ψ_l.

引理5.6 设 l 是一个奇素数，且 $l \neq p$, 有理函数 $f = u + vY \in k[E]$, 其中 $u, v \in k[X]$. 则下面的两个论断等价:

1. 对任意的 $P \in E[l]$ 都有 $f(P) = 0$.
2. ψ_l 在 $k[X]$ 中整除 u 和 v.

证明 首先由推论 3.54 知 $\psi_l \in k[X]$, 因此引理中的论断是有意义的. 由命题 3.57 可知

$$\operatorname{div}\psi_l = \langle E[l]\rangle - l^2\langle \mathcal{O}\rangle.$$

从而在 $E[l]$ 中 f 是零多项式的充分必要条件是 f/ψ_l 没有有限极点，再由命题 2.34 可知 $f/\psi_l \in k[E]$. 设 $f/\psi_l = a + bY$, 其中 $a, b \in k[X]$, 则 $f = u + vY = a\psi_l + b\psi_l Y$, 从而 $u = a\psi_l$, $v = b\psi_l$ 都能被 ψ_l 整除. □

利用上面的引理可知，检查 $E[l]$ 上一个关于多项式的恒等式是否成立，就归结为检查在该多项式的标准型 $f = u + vY$ 中 u, v 是否能被 ψ_l 整除. 如果该多项式有特殊的形式，那么这样的检查就可以更加简单.

引理5.7 设 l 是奇素数且 $l \neq p$, 有理多项式 $f \in k[E]$ 满足 $f \in k[X]$ 或 $f/\psi_2 \in k[X]$. 令

$$\widetilde{f} = \begin{cases} f, & f \in k[X], \\ \dfrac{f}{\psi_2}, & \text{其他}, \end{cases}$$

则下面两个论断等价:

1. *存在点* $P \in E[l]$, *使得* $f(P)=0$.
2. $\gcd(\widetilde{f},\psi_l)\neq 1$.

证明　首先假定 $f\in k[X]$, $P=(x,y)\in E[l]$ 满足 $f(P)=0$. 则在 $k[X]$ 中 $X-x$ 整除 f. 另一方面, $\psi_l(P)=0$, 因此在 $k[X]$ 中, $X-x$ 也整除 ψ_l, 从而 f 和 ψ_l 有非平凡的最大公因子. 类似地可以完成相反方向的证明.

假定 $f=\psi_2\widetilde{f}$, 其中 $\widetilde{f}\in k[X]$. 由于 l 是奇素数, 因而对任意的 $P\in E[l]$, 都有 $\psi_2(P)\neq 0$. 所以, 如果存在 l 阶扭点 P 满足 $f(P)=0$, 这等价于 $\widetilde{f}(P)=0$, 由前面的讨论可知, 在这种情况下结论仍然成立. □

在求解 (5.3) 时, 需要计算 φ^2+s. 为此, 我们需要先检查 $\varphi^2=\pm s$ 是否成立. 在 Schoof 最初的方法中, 首先利用引理 5.7 检查是否存在一个 l 扭点 P, 满足 $\varphi^2(P)=\pm sP$. 如果不存在, 那么就可以知道 $\varphi^2\neq\pm s$. 但是不幸的是, 由于引理 5.7 只是对特殊形式的多项式才有效, 因此这种方法需要区分特征是奇数和偶数的情况, 而且还要用到第 2 章表 2.2 中椭圆曲线的标准形式. 为此, 我们采用了另外一种处理方式: 由于引理 5.6 是对 $k[E]$ 中的所有多项式都成立, 从而不管是偶特征还是奇特征的情形, 我们都可以用统一的形式进行处理. 因此就可以检验 $\varphi^2(P)=\pm sP$ 是否对所有的 l 扭点 P 都成立.

1. 验证 $\varphi_l^2=\pm s$ 是否成立.

   $\varphi_l^2=\pm s$ 的一个必要条件是在 $E[l]$ 中 $X(\varphi^2)=X(s)$, 也就是说在 $E[l]$ 中 $X^{q^2}-g_s=0$. 由命题 3.52 和命题 3.51 的第 4 条可知

$$g_s=X-\frac{\psi_{s-1}\psi_{s+1}}{\psi_s^2}\in k(X),$$

   因此, 由引理 5.6 可知, 我们只需要验证

$$\psi_s^2(X^{q^2}-X)+\psi_{s-1}\psi_{s+1}\equiv 0 \pmod{\psi_l}$$

   是否成立即可. 如果上式不成立, 则 $\varphi_l^2\notin\{s,-s\}$, 从而可以采用第 2 步介绍的一般的加法公式. 如果上式成立, 我们需要区分下面两种情况: (1) 存在某个有限点 $P\in E[l]$, 使得 $\varphi_l^2(P)=-sP$;　(2)$\varphi_l^2=s$. 对于第一种情况, 要注意的是由于有可能存在有限点 P, $Q\in E[l]$, 满足 $\varphi_l^2(P)=-sP$, $\varphi_l^2(Q)=sQ$, 所以不一定有 $\varphi_l^2=-s$ 成立. 但是, 如果有限点 $P\in E[l]$, 满足 $\varphi_l^2(P)=-sP$, 代入公式 (5.2) 则有 $\mathcal{O}=\tau_0\varphi_l(P)$, 而 $\varphi_l(P)\neq\mathcal{O}$, 所以 $\tau_0=0$, 从而仍有 $\varphi_l^2=-s$. 于是如果上式成立, 我们有 $\varphi_l^2=-s$, 在这种情况下, 我们已经计算出 $\tau_0=0$ 或者 $\varphi_l^2=s$. 对于第二种情况, 有 $\tau_0\neq 0$, 而 (5.3) 表明

$$2s=\tau_0\varphi_l \iff \varphi_l=\frac{2s}{\tau_0}, \tag{5.4}$$

由于 $\tau_0 \neq 0$, l 是素数，因此上式中 τ_0 在 $\mathbb{Z}_l$ 中可逆是显然的. 将上式中 φ_l 代入到方程 (5.3) 中可得

$$\frac{4s^2}{\tau_0^2} + s = 2s \quad \Longleftrightarrow \quad \tau_0^2 = 4s.$$

因此 τ_0 是 $4s$ 在 $\mathbb{Z}_l$ 中的平方根. 我们首先要检查 s 是否为模 l 的二次剩余，即 $\left(\frac{s}{l}\right) = 1$ 是否成立. 如果 s 不是模 l 的二次剩余，则必有 $\varphi_l^2 = -s$ 且 $\tau_0 = 0$. 否则，令 ω 是 s 的一个平方根 (因 l 是比较小的素数，可用穷举的方法计算 ω). 由 (5.4) 可知

$$\varphi_l = \frac{2s}{\tau_0} = \frac{2\omega^2}{\pm 2\omega} = \pm\omega,$$

因此第二种情况可以通过检查等式 $\varphi_l = \pm\omega$ 是否成立来得到判定. 因此首先验证等式

$$\psi_\omega^2(X^q - X) + \psi_{\omega-1}\psi_{\omega+1} \equiv 0 \pmod{\psi_l} \tag{5.5}$$

是否成立. 如果不成立，则 $\varphi_l^2 = -s$, 从而 $\tau_0 = 0$. 否则，$\varphi_l^2 = s$, 然后通过检查第二个坐标来区分 $\varphi_l = \omega$ 和 $\varphi_l = -\omega$, 由命题 3.55 的第 2 条可知

$$h_\omega = Y + \frac{\psi_{\omega+2}\psi_{\omega-1}^2}{\psi_2\psi_\omega^3} - (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{\omega-1}\psi_{\omega+1}}{\psi_2\psi_\omega^2}.$$

约去分母可得

$$\begin{aligned}
&\psi_2\psi_\omega^3\big(Y(\varphi) - Y(\omega)\big)\\
=&\psi_2\psi_\omega^3(Y^q - h_\omega)\\
=&\psi_2\psi_\omega^3(Y^q - Y) - \psi_{\omega+2}\psi_{\omega-1}^2\\
&+ (3X^2 + 2a_2X + a_4 - a_1Y)\psi_{\omega-1}\psi_\omega\psi_{\omega+1},
\end{aligned} \tag{5.6}$$

然后消去 Y 的高次幂，得到一个多项式 $u + vY$, 其中 $u, v \in k[X]$. 如果 ψ_l 整除 u, v, 则 $\varphi_l = \omega$, $\tau_0 = 2\omega$, 否则 $\varphi_l = -\omega$, $\tau_0 = -2\omega$.

注 当特征是奇数时，则有更有效的表达形式：可选取具有 $a_1 = a_3 = 0$ 的标准形式，并且把命题 3.55 中的 h_ω 写成如下的简单形式

$$h_\omega = \frac{\psi_{\omega+2}\psi_{\omega-1}^2 - \psi_{\omega-2}\psi_{\omega+1}^2}{2\psi_2\psi_\omega^3}.$$

记

$$Y^q = Y(X^3 + a_2X^2 + a_4X + a_6)^{\frac{q-1}{2}},$$

则由定理 3.51 的第 4 条可知 $v=0$(即公式 (5.6) 中的最后结果 $\in k[X]$)，因此只需要验证一个多项式的除法就可以了. 目前，笔者还不知道对于一般的情形，能否避免第二个检验.

2. 如果第 1 步的检验失败，则 $\varphi_l^2 \neq \pm s$，因此 $\varphi^2 \neq \pm s$，我们可以使用一般的加法公式计算 φ^2+s：

$$\begin{aligned}
\alpha &= \psi_2\psi_s^3\big(Y(\varphi^2)-Y(s)\big)\\
&= \psi_2\psi_s^3(Y^{q^2}-h_s)\\
&= \psi_2\psi_s^3(Y^{q^2}-Y)-\psi_{s+2}\psi_{s-1}^2\\
&\quad +(3X^2+2a_2X+a_4-a_1Y)\psi_{s-1}\psi_s\psi_{s+1}, \qquad \text{(命题 3.55 的第 2 条)}\\
\beta &= \psi_2\psi_s^3\big(X(\varphi^2)-X(s)\big)\\
&= \psi_2\psi_s^3(X^{q^2}-g_s)\\
&= \psi_2\psi_s^3(X^{q^2}-X)+\psi_2\psi_{s-1}\psi_s\psi_{s+1}, \qquad \text{(命题 3.52)}
\end{aligned}$$

$$\begin{aligned}
\lambda &= \frac{\alpha}{\beta},\\
g_\varphi &= \psi_s^2\beta^2X(\varphi^2+s)\\
&= \psi_s^2\beta^2(-X^{q^2}-g_s+\lambda^2+a_1\lambda-a_2)\\
&= \psi_s^2\Big(\big((-X^{q^2}-X-a_2)\beta+a_1\alpha\big)\beta+\alpha^2\Big)+\beta^2\psi_{s-1}\psi_{s+1}, \qquad \text{(命题 3.52)}\\
h_\varphi &= \psi_s^2\beta^3Y(\varphi^2+s)\\
&= -\alpha(g_\varphi-X^{q^2}\psi_s^2\beta^2)-(Y^{q^2}+a_3)\psi_s^2\beta^3-a_1\beta g_\varphi\\
&= \psi_s^2\Big(-(Y^{q^2}+a_3)\beta+\alpha X^{q^2}\Big)\beta^2-(\alpha+a_1\beta)g_\varphi.
\end{aligned}$$

在后面的过程中，g_φ 和 h_φ 模 ψ_l 只需要计算一次. 然后对每一个 τ，$-(l-1)/2 \leqslant \tau \leqslant (l-1)/2$，我们验证是否有 $\varphi_l^2+s=\tau\varphi_l$，直至找到满足要求的 τ_0. 对于每个正值的 τ，计算

$$\begin{aligned}
&\psi_s^2\beta^2\psi_\tau^2(X^q,Y^q)\big(X(\varphi^2+s)-X(\tau\varphi)\big)=\\
&\qquad \psi_\tau^2(X^q,Y^q)g_\varphi-\psi_s^2\beta^2\big(\psi_\tau^2(X^q,Y^q)X^q-\psi_{\tau-1}(X^q,Y^q)\psi_{\tau+1}(X^q,Y^q)\big)
\end{aligned}$$

并检查它是否能被 ψ_l 整除. 注意到 $\gcd(\psi_s^2,\psi_l)=1$：如果 $s=0$，则是平凡的[①] 否则，有 $\gcd(s,l)=1$，从而有 $E[s]\cap E[l]=\{\mathcal{O}\}$，即 $E[s]\cap E[l]$ 中不包含有限

① 如果 $s=0$，这说明 $l|q$，即 $l=p$ 与 l 的选取矛盾 —— 译者注.

点.[1] 类似地，我们有

$$\gcd(\psi_\tau^2(X^q, Y^q), \psi_l) = \gcd(\psi_\tau^{2q}, \psi_l) = 1.$$

然而，β 可能在某个有限 l 扭点处取零值，即存在 $Q \in E[l]$ 满足 $\varphi^2(Q) = \pm sQ$. 但是，在这第 2 步中，至少存在一个有限点 $P \in E[l]$ 满足 $\varphi^2(P) \neq \pm sP$. 因此，如果上面的多项式能够被 ψ_l 整除，则对于这个点 P 有 $(\varphi^2 + s)(P) = \pm\tau\varphi(P)$. 由于 P 点也满足 (5.3) 式，即 $(\varphi^2 + s)(P) = \tau_0\varphi(P)$，且 $\varphi(P)$ 也是 l 阶点，因此 $\tau_0 \equiv \pm\tau \pmod{l}$. 为了区分 $\tau_0 = \tau$ 和 $\tau_0 = -\tau$，我们需要比较 Y 坐标，计算

$$\begin{aligned}
&\psi_s^2\beta^3\psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)\big(Y(\varphi^2 + s) - Y(\tau\varphi)\big) \\
=\ &\psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)h_\varphi \\
&- \psi_s^2\beta^3\big(\psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)Y^q + \psi_{\tau+2}(X^q, Y^q)\psi_{\tau-1}^2(X^q, Y^q)\big) \\
&+ \psi_s^2\beta^3\big(3X^{2q} + 2a_2X^q + a_4 - a_1Y^q\big)\psi_{\tau-1}(X^q, Y^q)\psi_\tau(X^q, Y^q)\psi_{\tau+1}(X^q, Y^q)
\end{aligned}$$

并检查其是否能够被 ψ_l 整除. 如果能够被 ψ_l 整除，则 $\tau_0 = \tau$，否则 $\tau_0 = -\tau$.

注 同样地，当域的特征为奇数时，由于多项式一定属于 $k[X]$ 或 $Yk[X]$，因此其他的整除性检查都可以省略. 对于一般的情形，我们希望分解除子多项式中的 ψ_2 的幂. 在计算过程中，合理地安排和存储中间结果是非常重要的，这些中间结果应该模去 ψ_l. 而在计算 X^q, X^{q^2}, Y^q 和 Y^{q^2} 时，总是用“平方–乘”的算法，而且还要不断地模去 ψ_l 和椭圆曲线 E.

为了方便，我们将算法总的描述如下：

算法5.8 (Schoof 算法) *下面的算法通过在域 k 中进行 $O(\log^6 q)$ 次乘法和求逆运算，以及存储 $O(\log^3 q)$ 个域元素，能够计算出 E_k 的阶.*

1. *确定一个不包含 2 和 p 的素数集合 $\mathcal{L}$，满足*

$$\prod_{l\in\mathcal{L}} l > 4\sqrt{q}.$$

进行预计算：利用命题 3.53 中的递归公式，对任意的 i，$2 \leqslant i \leqslant \max\mathcal{L}$，计算 ψ_i. 对每一个素数 $l \in \mathcal{L}$，利用下面的第 2 步至第 5 步计算 $\tau_0 \pmod{l}$.

2. *令 $s = q \bmod l$. 利用“平方–乘”算法计算*

$$X^q \bmod \psi_l, \quad X^{q^2} \bmod \psi_l, \quad Y^q \bmod (E, \psi_l), \quad Y^{q^2} \bmod (E, \psi_l).$$

---

[1] $\gcd(s, l) = 1$，则 $sx + ly = 1$. 如果 $P \in E[s] \cap E[l]$，则 $P = x(sP) + y(sP) = \mathcal{O} + \mathcal{O} = \mathcal{O}$——译者注.

3. 计算

$$\psi_s^2(X^{q^2}-X)+\psi_{s-1}\psi_{s+1} \bmod \psi_l.$$

如果结果不为零，则转到第4步. 否则计算 Legendre 符号 $\left(\frac{s}{l}\right)$. 如果 $\left(\frac{s}{l}\right)=-1$, 则 $\tau_0=0$; 否则通过穷举计算 $\omega\in\mathbb{Z}_l$ 满足 $\omega^2=s$. 计算

$$\psi_\omega^2(X^q-X)+\psi_{\omega-1}\psi_{\omega+1} \bmod \psi_l.$$

如果该多项式不为零，则 $\tau_0=0$. 否则检查等式

$$\psi_2\psi_\omega^3(Y^q-Y)-\psi_{\omega+2}\psi_{\omega-1}^2+(3X^2+2a_2X+a_4-a_1Y)\psi_{\omega-1}\psi_\omega\psi_{\omega+1} \bmod (E,\psi_l)=0$$

是否成立. 如果等式成立，则 $\tau_0=2\omega$, 否则 $\tau_0=-2\omega$. 如果在这一步可以计算出 τ_0, 则返回到第 2 步，对 $\mathcal{L}$ 中的下一个素数进行处理.

4. 利用命题 3.53 中的递推公式，对每一个 $i, 2\leqslant i\leqslant(l-1)/2$, 预计算 $\psi_i(X^q,Y^q)$, 实际上这就是 $\psi_i\circ\varphi$.

5. 计算下面的多项式 $\bmod(E,\psi_l)$:

$$\begin{aligned}
\alpha&=\psi_2\psi_s^3(Y^{q^2}-Y)-\psi_{s+2}\psi_{s-1}^2+(3X^2+2a_2X+a_4-a_1Y)\psi_{s-1}\psi_s\psi_{s+1},\\
\beta&=\psi_2\psi_s^3(X^{q^2}-X)+\psi_2\psi_{s-1}\psi_s\psi_{s+1},\\
g_\varphi&=\psi_s^2\Big(((-X^{q^2}-X-a_2)\beta+a_1\alpha)\beta+\alpha^2\Big)+\beta^2\psi_{s-1}\psi_{s+1},\\
h_\varphi&=\psi_s^2\Big(-(Y^{q^2}+a_3)\beta+\alpha X^{q^2}\Big)\beta^2-(\alpha+a_1\beta)g_\varphi.
\end{aligned}$$

对每一个 $\tau, 1\leqslant\tau\leqslant(l-1)/2$, 重复以下计算，直至找到满足条件的 τ_0:

$$\psi_\tau^2(X^q,Y^q)g_\varphi-\psi_s^2\beta^2\big(\psi_\tau^2(X^q,Y^q)X^q-\psi_{\tau-1}(X^q,Y^q)\psi_{\tau+1}(X^q,Y^q)\big) \bmod (E,\psi_l).$$

如果结果不为零，则对下一个 τ 进行计算；否则，计算

$$\begin{aligned}
&\psi_s^2\beta^3\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)\big(Y(\varphi^2+s)-Y(\tau\varphi)\big)\\
&=\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)h_\varphi\\
&-\psi_s^2\beta^3\big(\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)Y^q+\psi_{\tau+2}(X^q,Y^q)\psi_{\tau-1}^2(X^q,Y^q)\big)\\
&+\psi_s^2\beta^3\big(3X^{2q}+2a_2X^q+a_4-a_1Y^q\big)\psi_{\tau-1}(X^q,Y^q)\\
&\cdot\psi_\tau(X^q,Y^q)\psi_{\tau+1}(X^q,Y^q) \bmod (E,\psi_l).
\end{aligned}$$

如果结果不为零，则 $\tau_0=\tau$, 否则 $\tau_0=-\tau$.

6. 利用中国剩余定理，计算出满足下列条件的唯一的 $t\in[-2\sqrt{q},2\sqrt{q}]$ 且对任意的 $l\in\mathcal{L}$, 都有 $t\equiv\tau_0 \pmod l$. 则有 $|E_k|=q+1-t$.

为对 Schoof 算法进行复杂度分析，我们需要知道该算法中所必需的多项式基本运算的次数. 由于域 k 中的加法运算所需计算量相对是比较小的 (需要 $O(\log q)$

比特运算)，我们只考虑中乘法和求逆 (都需 $O(\log^2 q)$ 比特运算)，把它们作为域 k 的基本运算.

引理5.9 *设 f, g 是 $k[X]$ 中的多项式，$d_f = \deg f \geqslant \deg g = d_g$，$\alpha \in k$. 则下面多项式运算所需要的域 k 中的基本运算次数为：*

- *$f+g$ 所需要运算次数为零，*
- *αf 所需要的运算次数为 $O(d_f)$，*
- *fg 所需要的运算次数为 $O(d_f d_g)$，*
- *多项式 f 除以 g 取余数所需要的运算次数为 $O((d_f - d_g)d_g)$.*

证明 对于加法和纯量乘法该结论是平凡的. 对于 fg，只要注意到有 $(d_f+1)(d_g+1)$ 个项需要相乘和相加即可. 用通常的方法计算 $f = ag + b$ 时 (其中 $\deg b < d_g$)，所需要的计算量相当于计算 ag，其中 $\deg a = d_f - d_g$，具体的细节可参考 [Cohen, 1993], p.110. □

引理5.10 *设 f, g, h 是 $k[E]/(\psi_l)$ 中的约化形式，即 $f = f_1 + f_2 Y$，$g = g_1 + g_2 Y$，$h = h_1 + h_2 Y$，其中 f_1，f_2，g_1，g_2，h_1，$h_2 \in k[X]$，它们的次数不超过 $\deg \psi_l$，$\alpha \in k$. 则完成下面约化所需要的域 k 中的基本运算次数为：*

- *$f+g$ 所需要的运算次数为零，*
- *αf 所需要的运算次数为 $O(l^2)$，*
- *fg 所需要的运算次数为 $O(l^4)$.*

证明 注意到 ψ_l 的次数是 $(l^2-1)/2 \in O(l^2)$，前面两个结论是显然的. 为计算 fg，有

$$
\begin{aligned}
fg &= (f_1 + f_2 Y)(g_1 + g_2 Y) \\
&= f_1 g_1 + f_2 g_2 (X^3 + a_2 X^2 + a_4 X + a_6) \\
&\quad + (f_1 g_2 + f_2 g_1 - f_2 g_2 (a_1 X + a_3))Y.
\end{aligned}
$$

所以我们将要计算固定数目的次数为 $O(l^2)$ 的单变量多项式的乘积，由前面引理可知这需要 $O(l^4)$ 次域 k 中的基本运算. 最后还需要两次除法来得到模 ψ_l 的余数，被除的多项式次数为 $O(l^2)$，而同样地由引理可知这仍然需要 $O(l^4)$ 次域 k 中的基本运算，因此命题成立. □

算法 5.8 中复杂度的证明 在 Schoof 算法的步骤 1 中，建议使用 $\mathcal{L} = \{p_2, \cdots, p_n\}$ 是不等于 2 和 p 的前 $n-1$ 个素数. 为了简单起见，不妨设 p_i 为

第 i 个素数，下面估计 n 和 p_n 的大小. 选取的 n 必须满足

$$\prod_{i=2}^{n} p_i > 4\sqrt{q},$$

这等价于

$$\vartheta(p_n) := \log\left(\prod_{i=1}^{n} p_i\right) > \log(8\sqrt{q}).$$

由 [Rosser and Schoenfeld, 1962] 中第 70 页的结论可知

$$\vartheta(p_n) < p_n\left(1 + \frac{1}{2\log p_n}\right) < 2p_n,$$

因此，只要选择如下的 p_n 即可：

$$p_n \approx \frac{1}{2}\log\left(8\sqrt{q}\right) \in O\left(\log q\right).$$

所以诸 ψ_i 的计算可以在 $O(p_n) = O(\log q)$ 次多项式乘法和除法下完成，其中每个多项式的次数至多是 $(p_n^2 - 1)/2 \in O(\log^2 q)$，从而由引理 5.9 可知第 1 步中总的复杂度是 $O\left(\log^5 q\right)$. 对于单个素数 l 来说，在第 2 步中计算 X^q, X^{q^2}, Y^q 和 Y^{q^2} 模 ψ_l 需要 $O\left(\log q\right)$ 次 $k[E]/(\psi_l)$ 中的乘法运算. 由引理 5.10，该步中所需的总计算量是 $O\left(l^4 \log q\right)$. 在第 3 步中，需要计算的是 $k[E]/(\psi_l)$ 中常数次的乘法运算、Legendre 符号 $\left(\frac{s}{l}\right)$ 的计算以及用穷举的方法计算模 l 的平方根，其中第一部分需要 $O\left(l^4\right)$ 次基本运算，并且与其他两部分相比占支配地位 (即剩下两部分的计算可以忽略不计). 在第 4 步中要计算一系列关于 X^q 和 Y^q 的除子多项式 $\psi_i(X^q, Y^q)$，这需要 $O(l)$ 次 $k[E]/(\psi_l)$ 中的乘法，从而需要 $O(l^5)$ 次域 k 中的基本运算. 在第 5 步中，对每一个 τ，需要常数次 $k[E]/(\psi_l)$ 中的乘法运算，即 $O(l^4)$ 次域 k 中的基本运算. 从而完成第 5 步所需时间是 $O(l^5)$. 考虑到 $l \in O(\log q)$，以及第 2 步到第 5 步需重复 $|\mathcal{L}| \in O(\log q)$ 次，因此该算法总共需要 $O\left(\log^6 q\right)$ 次域 k 中的基本运算，当然第 6 步中利用中国剩余定理所需的计算量可以忽略不计.

我们需要存储 $O\left(\log q\right)$ 个除子多项式和常数多个次数最多是 l^2 的多项式，所以总空间复杂度是 $O\left(\log^3 q\right)$. □

注 该算法的计算复杂度是 $O\left(\log^6 q\right)$ 次域运算，相当于 $O\left(\log^8 q\right)$ 次比特运算. 在 Schoof 的原始算法中，计算复杂度是 $O\left(\log^9 q\right)$ 次比特运算，原因是它对每一个 i，独立地利用 "平方–乘" 的方法计算除子多项式

$$\psi_i(X^q, Y^q) = \left(\psi_i(X, Y)\right)^q \bmod \psi_l.$$

因此在 Schoof 的算法中，每一次多项式除法都需要 $O\left(\log q\right)$ 次 $k[E]/(\psi_l)$ 中的乘法. 而用我们这里采用的技巧，在每次多项式除法中，只需要 $O(1)$ 次 $k[E]/(\psi_l)$ 中

的乘法，这一点已经由几个作者彼此独立地提到过. 进一步，对于每一个除子多项式 ψ_l，在计算 $\psi_i(X^q,Y^q)$ 时，如果采用预先计算 $X^q \bmod \psi_l$, $Y^q \bmod \psi_l$ 的方法，可将整个计算量降到 $O(\log^2 q)$ 次 $k[E]/(\psi_l)$ 中的乘法.

Müller 曾对 q 是大素数的情形实现了这个算法. 他选择的素数集合为 $\mathcal{L} = \{3,\ 5,\ 7,\ 11,\ 13\}$，但是在计算 $l = 17$ 的时候失败了，细节可参阅 [Müller, 1991], p.106. 这时相对应的 q 大概为

$$\left(\frac{3\cdot 5\cdot 7\cdot 11\cdot 13}{4}\right)^2 \approx 2^{24}.$$

为了使 Schoof 算法更有利于实用，Buchmann 和 Müller 建议将 Schoof 算法和 Shanks 的大步–小步的算法结合起来. 第一步，先利用 Schoof 算法，计算 t 模一个素数集 $\mathcal{L}$，因此可得到 $t \equiv l_1 \pmod L$，其中 $L = \prod_{l\in\mathcal{L}} l$. 接着执行 Shanks 算法的第一步：随机选择点 P，再以 $C = q+1-2\sqrt{q}$，$B = q+1+2\sqrt{q}$ 为初始值调用算法 5.3，以 L 和 l 来决定满足

$$rP = \mathcal{O}, \quad r \equiv l_1 \pmod L.$$

的 $r \in [C, B]$. 由于 $r = |E_k|$ 满足该条件，因此算法 5.3 一定能够找到匹配. 如果找到的匹配是唯一的，则这就是 $|E_k|$. 否则，该算法的第二个输出就是 $\mathrm{ord}(LP)$，又由于 P 点的阶 $\mathrm{ord}P | L\cdot \mathrm{ord}(LP)$，因此可以利用算法 5.2 计算出 $\mathrm{ord}P$. 一直调用这个算法，直到找到满足 $\mathrm{ord}P \geqslant \sqrt{q}-1$ 的点 P. 然后再利用 Shanks 算法的第 2 步和第 3 步，来计算第二个点 P' 的阶. 糟糕的是，Schoof 算法所得到的信息在 Shanks 算法的第二阶段 (即第 4 步) 没什么用处，但是在实际应用中，这一步并不是经常发生的，因此并不会带来多严重的危害. 注意，在长度为 $4\sqrt{q}$ 的区间 $[q+1-2\sqrt{q},\ q+1+2\sqrt{q}]$ 中，最多只有四个可能的 $|E_k|$ 值，它们是 $\mathrm{ord}P \geqslant \sqrt{q}-1$ 的倍数.

当固定一个素数集 $\mathcal{L}$ 时，上述改进算法的计算复杂度和原始的 Shanks 算法的计算复杂度相当. 该算法的计算记录可参见文献 [Müller, 1991], p.107，其中 q 大约是 $5\cdot 10^{32}$.

5.3 Elkies 素数

虽然 Schoof 算法是个多项式时间的算法，但是由于除子多项式次数的快速增长，使得 Schoof 算法的计算复杂度的次数较高，从而导致该算法对于比较大的域来说，实现起来比较困难. Atkin 和 Elkies 在他们还没有发表的论文中对该算法提

出了改进，这就是后面几节我们要讨论的话题. 最近，Elkies 在 [Elkies, 1998] 中解释了他的思想，更好的参考文献是 [Müller, 1995], [Schoof, 1995], [Lercier, 1997a], 而且在这些文献里还能够找到这里我们不得不省略的一些细节.

和以前一样，令 E 表示定义在域 $k=\mathbb{F}_q$ 上的椭圆曲线，$K=\overline{k}$ 是 k 的代数闭包. 令 l 是不同于 p 的奇素数. 回忆 Frobenius 自同态在 $E[l]$ 上的限制 φ_l 满足下面的方程

$$\varphi_l^2-\tau_0\varphi_l+s=0, \tag{5.7}$$

其中 $s\equiv q \pmod{l}$. 我们需要计算 φ_l 的迹 τ_0. Elkies 所做改进的基本思想是：利用除子多项式的一个次数比较小的因子来代替 ψ_l 进行计算. 由于 ψ_l 是 $\mathbb{Z}[X,a_1,a_3,a_2,a_4,a_6]$ 中不可约多项式，因此它没有 "通用" 的因子. 我们只能将给定椭圆曲线的具体参数 a_i 代入到 ψ_l 中，来得到所需要的因子. 一般地说，我们可以分解除子多项式，但是，这又涉及到大量费时的模 ψ_l 的计算.

回忆一下，如果 $E[l]=S\,\dot\cup\,\overline{S}\,\dot\cup\,\{\mathcal{O}\}$①，则

$$\psi_l=\prod_{P\in S}\big(X-X(P)\big).$$

我们考虑 $E[l]$ 中所有的非平凡子群 C，易知，它们恰好是椭圆曲线 E 中所有 l 阶点所生成的循环子群. 称这样的子群为 *l 群*. 在一般的群论中，l 群通常指的是阶为 l 的幂次的群. 类似于除子多项式的定义，我们定义如下的多项式

$$f_C=\prod_{P\in S_C}\big(X-X(P)\big)\in K[X],$$

其中 $S_C:=S\cap C$，因此 $C=S_C\,\dot\cup\,\overline{S_C}\,\dot\cup\,\{\mathcal{O}\}$. 由定义可知，在 $K[X]$ 中，f_C 是 ψ_l 的因子. 但是只有当 f_C 落在 $k[X]$ 中的时候，才在我们的计算上有用.

命题5.11　下面的论断是等价的：

1. $f_C\in k[X]$;
2. $\varphi_l(C)\subseteq C$;
3. $\varphi_l(C)=C$, 即 C 在Frobenius自同态的作用下不变;
4. C 是线性变换 φ_l 在某个特征值 $\alpha\in\mathbb{Z}_l^{\star}$ 所对应的特征子空间.

证明　由于 φ_l 是单射，而且 C 是有限集，因此论断 2 和论断 3 是等价的.

① 由于 l 是奇素数，$E[l]$ 中没有 2 阶点，因此对于 $E[l]$ 中所有有限点进行分类：如果 $P\in S$，则 $-P\in\overline{S}$—— 译者注.

令 $\varphi_{K/k}$ 表示域 K/k 中的 Frobenius 自同构，也表示它在 $K[X]$ 中的典范扩张，即

$$\varphi: \quad \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i^q X^i.$$

则 $f_C \in k[X]$ 等价于 $\varphi_{K/k}(f_C) = f_C$. 由于

$$\varphi_{K/k}(f_C) = \prod_{P \in S_C} (X - X(P)^q) = \prod_{P \in S_C} \Big(X - X\big(\varphi_l(P)\big)\Big),$$

这意味着 φ_l 将 C 中点的 X 坐标进行置换，从而 φ_l 保持 C 不变，这就证明了论断 1 和论断 3 的等价性.

最后证明论断 3 和论断 4 的等价性. 由于 C 是循环群，设 P 为 C 的生成元，则 $\varphi_l(C) = C$ 就意味着 φ_l 将 P 映射到 C 的另外一个生成元 P'，而 P' 一定形如 αP，其中 $\alpha \in \mathbb{Z}_l^\times$. 注意由于 φ_l 是单射，因此零不可能是 φ_l 的特征根. □

因此，如果存在在 Frobenius 自同态作用下保持不变的 l 群 C，或者等价地说，如果 φ_l 有一个特征根 $\alpha \in \mathbb{Z}_l$，则除子多项式 ψ_l 就有一个次数为 $(l-1)/2$ 的因子 $f_C \in k[X]$.

目前我们暂且假定存在这样一个多项式 f_C，那么对任意的 $\alpha \in \{1, \cdots, (l-1)/2\}$，我们可以通过检查在 C 上是否有 $\varphi_l = \pm\alpha$，来确定 φ_l 的特征根. 这一过程可以采用和 Schoof 算法第 1 步完全相同的方法，唯一的区别就是所有的计算都是模 f_C，而不是模 ψ_l. 如果我们知道了 α，就可以很容易计算出 τ_0：如果 P 是对应 α 的特征向量，则 (5.7) 式表明

$$\mathcal{O} = \big(\varphi_l^2 - \tau_0\varphi_l + s\big)(P) = \big(\alpha^2 - \tau_0\alpha + s\big)P,$$

由于点 P 的阶为 l，因此在 $\mathbb{Z}_l$ 中有 $\alpha^2 - \tau_0\alpha + s = 0$. 所以

$$\tau_0 = \alpha + s\alpha^{-1},$$

其中 α^{-1} 表示 α 在 $\mathbb{Z}_l$ 中的逆.

为了完成上面描绘的算法，我们需要解决两个问题：第一，如何判断一个素数 l 为 Elkies 型素数，即 φ_l 在 $\mathbb{Z}_l$ 中有特征根？很自然地，这意味着 φ_l 的特征多项式 $X^2 - \tau_0 X + s$ 在 $\mathbb{Z}_l$ 中有根，这相当于说 $\tau_0^2 - 4s$ 要么模 l 为零[①]，要么是模 l 的二次剩余. 应该有一半的素数 l 能够满足这情况，但是由于我们并不知道 τ_0 到底是多少，因此前面的判断原则对于我们来说毫无用处. 第二，如何在不分解 ψ_l 的前提下，计算多项式 f_C？我们将在 5.4 节中解决上面这两个问题. 另外，我们将在 5.5 节中说明，即使 φ_l 在 $\mathbb{Z}_l$ 中没有特征根，我们仍然可以得到 τ_0 的若干信息. 最后，在 5.6 节中，我们将完整地描绘出 SEA 算法，并给出若干实验数据.

① 原文误为 $\tau_0 - 4s$—— 译者注.

5.4　同种映射和模多项式

这一节我们将回答下面的问题：是否存在 l 群 C，使得它在 Frobenius 自同态的作用下不变. 最后的结果表明，Frobenius 自同态在 C 上的作用，可由椭圆曲线 E/C 的 j 不变量来描述，并且存在一个从 E 到 E/C 的同种映射，它的核为 C. 最后，问题归结为判断一个多项式是否在 $k[X]$ 中有根. 这一节中大部分结果的证明已经超出了本书的范围，而且最后关于除子多项式 ψ_l 的因子 f_C 的计算，也超出了本书的范围，这需要一些关于复数域上椭圆曲线和模形式方面的基本知识.

我们在 3.1 节中介绍了定义在同一条椭圆曲线上的有理映射和同种映射的概念，下面把这两个概念推广到定义在不同椭圆曲线之间的情形.

定义5.12　*设 E 和 E' 是定义在 k 上的椭圆曲线. 从 E 到 E' 的有理映射是一个有理函数对 $\alpha \in K(E) \times K(E)$，满足 E' 的方程，即 $E' \circ \alpha = 0$. 换句话说就是，有理映射是椭圆曲线 $E'_{K(E)}$ 上的一个点. 称一个有理映射是定义在域 k 上的，是指它确实落在 $E'_{k(E)}$ 中. 如果一个有理映射同时还是一个群同态，则称为同种映射. 如果存在一个从 E 到 E' 的同种映射，则称 E 和 E' 是同种的. 如果该同种映射还是定义在 k 上的，则称它们是 k 同种.*

可以作为一些简单的练习来证明 3.1 节和 3.2 节的一系列结论，对于以上广义的同种映射仍然成立，所做的只是在适当的地方把 E 替换为 E'，把 P 替换为 P'. “是同种的” 这一概念是有意义的，因为它定义了一个等价关系. 在等价关系的三条性质中，只有对称性是不平凡的，这可以证明如下：设 $\alpha: E \to E'$ 是次数为 m 的同种映射，则存在同种映射 $\widehat{\alpha}: E' \to E$，满足 $\widehat{\alpha} \circ \alpha = [m]$，其中 $\widehat{\alpha}$ 就是所谓的对偶同种. 想进一步了解细节的读者，可参阅 [Silverman, 1986] 的第 III.6 节.

由于同种映射 (α_1, α_2) 的核是由 α_1 或 α_2 的极点构成 (可参阅第三章中定义 3.1 后面的注释)，再由推论 2.30 知，一个有理函数最多只可能有有限多个极点，因此任何非零同种的核一定是有限集. 反之，Vélu 在 [Vélu, 1971] 中证明了：对于 E 的任意有限子群 C，一定存在一条椭圆曲线 E' 和一个同种映射 $\alpha: E \to E'$，α 的核为 C，而且 E' 在同构的意义下是唯一的. 这个同种映射 α 可如下给出：

$$\alpha_1(P) = X(P) + \sum_{Q \in C \setminus \{\mathcal{O}\}} \big(X(P+Q) - X(Q)\big),$$

$$\alpha_2(P) = Y(P) + \sum_{Q \in C \setminus \{\mathcal{O}\}} \big(Y(P+Q) - Y(Q)\big),$$

如果采用 3.1 节的记号就是

$$\alpha_1 = \sum_{Q\in C} X\circ\tau_Q - c_1, \qquad \alpha_2 = \sum_{Q\in C} Y\circ\tau_Q - c_2,$$

其中

$$c_1 = \sum_{Q\in C\setminus\{\mathcal{O}\}} X(Q)\in K, \qquad c_2 = \sum_{Q\in C\setminus\{\mathcal{O}\}} Y(Q)\in K.$$

由后面的公式可知 α_1 和 α_2 确实是有理函数, 由引理 3.14 和引理 3.16 知 τ_Q 是非分歧的, 从而它们恰好分别以 C 中的点作为 2 阶和 3 阶极点. α_1 和 α_2 的首项系数满足 $l(\alpha_1)=l(\alpha_2)=1$, 因此 $\alpha_2^2-\alpha_1^3$ 在极点 $\mathcal{O}$ 处阶最多是 5(可参阅第 3 章定义 3.40 后面的注释), 如果该极点的阶恰好为 5, 则 $\alpha_2^2-\alpha_1^3-l(\alpha_2^2-\alpha_1^3)\alpha_1\alpha_2$ 在极点 $\mathcal{O}$ 处的阶最多为 4, 继续加上 $\alpha_1^2, \alpha_2, \alpha_1$ 和 1 的适当倍数可知, 存在一个有理函数

$$E'(\alpha_1,\alpha_2) = \alpha_2^2 + a_1'\alpha_1\alpha_2 + a_3'\alpha_2 - \left(\alpha_1^3 + a_2'\alpha_1^2 + a_4'\alpha_1 + a_6'\right)$$

以 $\mathcal{O}$ 为零点. 由 C 中的点 Q 产生的平移变换 τ_Q 保持 α_1 和 α_2 不变, 这说明 $E'(\alpha_1,\alpha_2)$ 以 C 中所有的点为零点, 从而没有极点. 由命题 2.34 和推论 2.35 可知, $E'(\alpha_1,\alpha_2)$ 是常值函数, 因此一定是零. 可以证明 E' 是非奇异的, 因此 E' 定义了一条椭圆曲线, 再由 $E'\circ\alpha=0$ 可知 α 是有理映射. 最后, α 把 $\mathcal{O}$ 映到 $\mathcal{O}$, 这说明 α 是同种映射 (证明可参阅 [silverman, 1986] 的第 III.4 节).

利用第 2 章中表 2.3 的加法公式, 可以得出 $X\circ\tau_Q$ 和 $Y\circ\tau_Q$ 的有理表达式, 从而可计算出同种映射和 E' 的明确表达式. 整个计算过程可能很繁琐, 但是很初等, 我们在这里只给出最后的结果. 令 $C = S\dot\cup\overline{S}\dot\cup R\dot\cup\{\mathcal{O}\}$, 其中 $R=\left(E[2]\cap C\right)\setminus\{\mathcal{O}\}$. 我们采用下面的记号 (也可参考 3.2 节):

$$\begin{aligned}
DX &= 2Y + a_1X + a_3,\\
DY &= 3X^2 + 2a_2X + a_4 - a_1Y,\\
t(Q) &= \begin{cases} DY(Q), & Q\in R,\\ (2DY + a_1DX)(Q), & Q\in S\cup\overline{S},\end{cases}\\
u(Q) &= (DX)^2(Q),
\end{aligned}$$

$$t = \sum_{Q\in S\cup R} t(Q),$$

$$u = \sum_{Q\in S\cup R}\left(u(Q) + X(Q)t(Q)\right).$$

因为对任意的 $Q \notin E[2]$，都有 $t(Q) = t(\overline{Q})$, $u(Q) = u(\overline{Q})$，因此上面的公式与 S 的选择无关. 于是有

$$
\begin{aligned}
\alpha_1 &= X + \sum_{Q \in S \cup R} \left(\frac{t(Q)}{X - X(Q)} + \frac{u(Q)}{(X - X(Q))^2} \right), \\
\alpha_2 &= Y - \sum_{Q \in S \cup R} \left(u(Q) \frac{DX}{(X - X(Q))^3} + t(Q) \frac{a_1(X - X(Q)) + Y - Y(Q)}{(X - X(Q))^2} \right. \\
&\quad \left. + \frac{a_1 u(Q) + DX(Q)DY(Q)}{(X - X(Q))^2} \right),
\end{aligned} \tag{5.8}
$$

$$
\begin{aligned}
a_1' &= a_1, \\
a_3' &= a_3, \\
a_2' &= a_2, \\
a_4' &= a_4 - 5t, \\
a_6' &= a_6 - (a_1^2 + 4a_2)t - 7u,
\end{aligned}
$$

c_1 和 c_2 实际上可以任意选择，我们的选择只是为了能够方便地推导出上面的计算公式.

设 C 是一个 l 群，令 E/C 表示满足下列条件的一条椭圆曲线：存在一个从 E 到 E/C 的同种映射，该同种映射的核为 C. 令 j/C 为 E/C 的 j 不变量. 由于 E/C 在同构的意义下是唯一的，因此，再由第 2 章中表 2.1 可知，$j/C \in K$ 是定义良好的[①]. 下面的定理表明，C 在 Frobenius 自同态幂的作用下的不变性与 j/C 密切相关：

定理5.13　设 E 是定义在 k 上的非超奇异椭圆曲线，且它不与某一条 j 不变量是 0 或 1728 的椭圆曲线 k 同种. 令 C 是一个 l 群，则对于正整数 d，下面两个论断等价：

1. $\varphi_l^d(C) = C$,
2. $j/C \in \mathbb{F}_{q^d}$.

证明　先假定 φ_l^d 是 C 上的一个双射. 由前面的公式可知，只要证明 t, $u \in \mathbb{F}_{q^d}$ 就可以了，这样的话，就有 $a_i' \in \mathbb{F}_{q^d}$，从而 j/C 也是 $\mathbb{F}_{q^d}$ 中的元素. 因此我们需

---

① 即满足前面条件的椭圆曲线 E/C 可能不唯一，但是它们的 j 不变量是相同的，或者说 j/C 与 E/C 的选择无关 —— 译者注.

要验证 $t^{q^d}=t$, $u^{q^d}=u$.

$$t^{q^d}=\sum_{Q\in S\cup R}t(Q)^{q^d}=\sum_{Q\in S\cup R}t\big(\varphi_l^d(Q)\big)=\sum_{Q\in\varphi_l^d(S)\cup\varphi_l^d(R)}t(Q).$$

在最后一个等号中，我们利用了 Frobenius 自同态保持点的阶不变. 根据假设，φ_l 诱导 C 上的一个置换，因此 $\varphi_l^d(R)=R$(事实上，因 l 是奇数，故 $R=\varnothing$)，且 $C=\varphi_l^d(S)\,\dot\cup\,\overline{\varphi_l^d(S)}\,\dot\cup\,R\,\dot\cup\,\{\mathcal{O}\}$，这表明 $t^{q^d}=t$，几乎完全一样的方法可证明 $u^{q^d}=u$.

为了证明相反的方向，我们需要了解椭圆曲线自同态环的更多知识，这些内容超出了本书的范围，感兴趣的读者可参阅 [Müller, 1995] 中的第 3.10 节. □

上面的定理表明，存在在 Frobenius 自同态的作用下保持不变的 l 群的充分必要条件是：多项式 $\prod_{C\text{是 }l\text{ 群}}(X-j/C)$ 在域 k 中有根. 我们可以在不计算出 j/C 的情况下把这个多项式计算出来.

定理5.14 *存在多项式 $\Phi_l\in\mathbb{Z}[X,Y]$ 满足下面的性质：如果 E 是定义在 k 上的非超奇异椭圆曲线，它的 j 不变量不等于 0 和 1728，则*

$$\Phi_l\big(X,j(E)\big)=\prod_{C\text{是 }l\text{ 群}}\big(X-j/C\big).$$

而且，$\Phi_l\big(X,j(E)\big)$ 是 $l+1$ 次多项式且没有重根. 称 Φ_l 为 l 次模多项式.

证明 参阅 [Müller, 1995] 中的第 4.13 节和引理 4.14. 在那里，证明了特征 $p>3$ 的情形及特征 $p=2$ 和 $p=3$ 的情形. 类似于除子多项式，人们首先证明了复数域上椭圆曲线情形下，模多项式的分解特性，接着证明了这个分解特性对于模 p 的情形也是正确的. 例如，关于次数的论断：我们知道，一共有 $l+1$ 个不同的 l 群，有 $l^2-1=(l-1)(l+1)$ 个阶为 l 的点，这些点就是所有 l 群的生成元，而每一个 l 群都有 $l-1$ 个生成元. □

推论5.15 *如果 E 是域 k 上的一条非超奇异椭圆曲线，且不与某一条 j 不变量等于 0 或 1728 的椭圆曲线 k 同种，则在 φ_l^d 下保持不变的 l 群的数目是*

$$\deg\left(\gcd\left(X^{q^d}-X,\Phi_l\big(X,j(E)\big)\right)\right).$$

证明 由定理 5.13 知，在 φ_l^d 作用下保持不变的 l 群的数目等于 $j/C\in\mathbb{F}_{q^d}$ 的 j 不变量的个数. 由定理 5.14 可知，后者恰好是多项式 $\Phi_l\big(X,j(E)\big)$ 在 $\mathbb{F}_{q^d}$ 中 (不相同的) 根的个数. 在有限域中有一个很重要的恒等式

$$X^{q^d}-X=\sum_{x\in\mathbb{F}_{q^d}}\Big(X-x\Big).$$

由此可知结论成立. □

这就回答了上节提出的第一个问题，即如何判断一个素数 l 为 Elkies 型素数. 在实际计算中，模多项式的计算非常耗时，它涉及到某一类模形式的 Fourier 级数展开，感兴趣的读者可参阅 [Müller, 1995] 的第 4 章和第 5 章. 然而，模多项式只需要计算一次，然后把它们存储在磁盘上. 在实际应用中，模多项式有两个缺点：第一，它关于 Y 的次数比较高 (事实上，模多项式是关于 X 和 Y 的对称多项式)，因此需要存储的系数比较多. 第二，模多项式的系数非常大. 例如，下面的 3 次模多项式取自 [Schoof, 1995] 中的第 236 页：

$$\begin{aligned}\Phi_3(X,Y) =& X^4+Y^4-X^3Y^3+2232(X^3Y^2+X^2Y^3)\\&-1069956(X^3Y+XY^3)+36864000(X^3+Y^3)\\&+2587918086X^2Y^2+8900222976000(X^2Y+XY^2)\\&+452984832000000(X^2+Y^2)-770845966336000000(X^2Y+XY^2)\\&+1855425871872000000000(X+Y).\end{aligned}$$

这个问题可以通过使用等价的多项式来解决，将 Y 用 $j(E)$ 代替后，等价模多项式与原来的模多项式有相同的分解类型. 下面是 $l=3$ 和 $l=13$ 时的等价模多项式：

$$\begin{aligned}G_3(X,Y) =& X^4+36X^3+270X^2+(-Y+756)X+729,\\G_{13}(X,Y) =& X^{14}+26X^{13}+325X^{12}+2548X^{11}+13832X^{10}+54340X^9\\&+157118X^8+333580X^7+509366X^6+534820X^5\\&+354536X^4+124852X^3+15145X^2+(-Y+746)X+13.\end{aligned}$$

一旦知道了素数 l 是 Elkies 型，即存在一个在 φ_l 的作用下不变的 l 子群 C，那么，我们可以从同种映射 $\alpha: E\to E/C$ 的明确表达式，得到我们需要的除子多项式 ψ_l 的因子 f_C. 由于 α_1 的分母恰好以 C 中的点为 2 阶极点，直线 $X-X(P)$ 对应的除子为 $\langle P\rangle+\langle\overline{P}\rangle-2\langle\mathcal{O}\rangle$(可参阅第 2 章中定义 2.27 后面的例子)，因此 α_1 的分母与

$$\prod_{P\in S}\Big(X-X(P)\Big)^2=f_C^2$$

最多相差一个常数因子，其中 $C=S\,\dot\cup\,\overline{S}\,\dot\cup\,\{\mathcal{O}\}$.

有多种不同的方法计算同种映射，我们在这里作简单的介绍，并提供相应的参考文献. 比较好的综述是 [Lercier, 1997a] 的第 4 章到第 8 章，算法复杂度方面的论断可参阅 [Lercier and Morain, 1997], p.13. 注意，从原则上说，这个问题可由 Vélu

公式 (5.8) 得到解决，可是我们希望有一个不依赖于 C 的具体细节的算法. Elkies 的方法最初是计算复数域上椭圆曲线的，再利用模 p 的方法，将这些结果推广到有限域上，细节可参阅 [Müller, 1995] 的第 6 章和第 7 章，该算法的计算复杂度为 $O(l^2)$. 在这个算法中，利用的椭圆曲线是标准形式 $Y^2 = X^3 + a_4X + a_6$，这就限制了有限域的范围，即域的特征 $p \notin \{2,3\}$. 还有一点就是，可能出现的有理数的分母可能是小素数的倍数，所以必须要求 $p > l$. 因此 Elkies 的方法非常适合很大的素数域. Couveignes 提出了一种基于所谓的椭圆曲线 "形式群"(formal group) 的算法 (参见 [Coureignes, 1994])，该算法对于任意的特征都是适用的，但是它的计算复杂度是 $O(l^3)$. 紧接着 Lercier 针对 $p = 2$ 的情况提出了一个方法，虽然运行时间与 Couveignes 的算法大致相同，但在实际运行中还是比较快的 (参见 [Lercier, 1996])，而且概念上比较简单. 最后，Couveignes 找到了一个新算法，其复杂度是 $O(l^{2+\varepsilon})$，对任意的 $\varepsilon > 0$ 成立. 该算法适用于任意特征的情况，而且从实现方面来看也是可行的 (参见 [Couveignes, 1996]).

5.5 Atkin 素数

即使没有在 φ_l 作用下保持不变的 l 群，我们仍然可以得到一些关于 τ_0 的信息. 命题 5.11 表明，此时 φ_l 的特征多项式 $X^2 - \tau_0 X + s$ 在 $\mathbb{Z}_l$ 中无根，或者说判别式 $\tau_0^2 - 4s$ 是模 l 的二次非剩余. 那么 $X^2 - \tau_0 X + s$ 在 $\mathbb{F}_{l^2}$ 中有两个不同的根 α 和 α^l. 我们现在感兴趣的是使得 φ_l^d 保持 l 群不变，或者说 φ_l^d 的特征根在 $\mathbb{Z}_l$ 中的最小正整数 d, . 基于 3.9 节的讨论，我们知道 φ_l^e 的特征多项式是 $(X-\alpha^e)(X-\alpha^{le})$. 当 $\alpha^e = (\alpha^e)^l$，即 $(\alpha^{l-1})^e = 1$ 时，该多项式的根在 $\mathbb{Z}_l$ 中. 因此，使 l 群保持不变的 φ_l 的最小幂，恰好是 α^{l-1} 在 $\mathbb{F}_{l^2}^\times$ 中的阶 d. 进一步地，由于 φ_l^d 有两个相同的特征根 $\alpha^d = \alpha^{dl}$，而 φ_l 有两个不相同的特征根 $\alpha \neq \alpha^l$，因此 φ_l^d 的若当标准型是对角矩阵，且所有的 l 群都在 φ_l^d 的作用下保持不变. 在推论 5.15 的假设下，整数 d 可作为满足 $\Phi_l\big(X, j(E)\big)$ 整除 $X^{q^d} - X$ 的最小整数来计算得到. 令 $\alpha^{l-1} = \zeta_d$ 是 $\mathbb{F}_{l^2}$ 中的 d 次本原单位根，则有 $\varphi(d)$ 个这样的 ζ_d，这里 φ 是 Euler 函数. 由于 $(\alpha^{l-1})^{l+1} = \alpha^{l^2-1} = 1$，因此 $d|l+1$，从而 $\varphi(d) \leqslant \varphi(l+1) \leqslant (l+1)/2$. 如果知道了 $\mathbb{F}_{l^2}$ 的一个本原元 g，即 $\mathbb{F}_{l^2}^\times = \langle g \rangle$，则可以将所有可能的 ζ_d 计算出来. 所有的 d 次本原单位根的集合为

$$\left\{ g^{\frac{l^2-1}{d}i} : \gcd(d,i) = 1 \right\}.$$

虽然在一般的情况下，求解有限域的本原元素是很困难的，但现在的情况是由于使用的 l 比较小，因此利用试的方法就可以了. 而且这些 ζ_d 只需要计算一次，然后保

存在磁盘上即可. 比较下面等式的系数:

$$X^2 - \tau_0 X + s = \left(X - \alpha\right)\left(X - \alpha^l\right)$$

可知

$$\tau_0 = \alpha + \alpha^l = \alpha(1 + \zeta_d),$$

因此

$$\tau_0^2 = \alpha^2\left(1 + \zeta_d\right)^2, \quad s = \alpha^{l+1} = \alpha^2\zeta_d.$$

这意味着

$$\tau_0^2 = \frac{s}{\zeta_d}\left(1 + \zeta_d\right)^2 = s\left(\frac{1}{\zeta_d} + 2 + \zeta_d\right).$$

这说明, ζ_d 和 ζ_d^{-1} 能够产生相同的 τ_0^2, 因此有 $\varphi(d)/2$ 个可能的 τ_0^2 和 $\varphi(d)$ 个可能的 τ_0.

5.6　SEA 算法

利用 5.3~5.5 节的结果以及所做的准备工作, 能够给出一个完整的算法. 首先, 我们需要验证推论 5.15 中的假设是否成立.

1. 测试超奇异性

由定义 3.71 可知, 特征为 2 或 3 的椭圆曲线 E 是超奇异的当且仅当 $j(E) = 0$. 对于其他的情形, 定理 3.72 表明, $|E_k|$ 可能的值最多有五个. 我们可以利用算法 5.1 在 E_k 中随机找一个点 P, 然后计算 kP(这里 k 为定理 3.72 中的五个可能值), 如果都不等于 $\mathcal{O}$, 则 E 不可能是超奇异的. 否则, E 很可能就是超奇异椭圆曲线, 由 4.5 节可知, 在密码学应用中最好不使用这种椭圆曲线.

2. 测试是否和 $j \in \{0,\ 1728\}$ 的椭圆曲线同种

假定 E 与 E' 是 k 同种的椭圆曲线, 在 5.4 节中, 我们描述了如果由同种映射 α 来明确地构造出 E', 这个过程递归地表明, 对于 $i = 1, 2, 3, 4, 6$, a_i' 是 $k[\alpha_1, \alpha_2, a_1', \cdots, a_{i-1}']$ 中某个多项式的首项系数, 因此 E' 是定义在 k 上的椭圆曲线. 假定 E' 的 j 不变量是 0 或者 1728, 下面的定理告诉我们, 如何计算 $|E_k|$ 的可能候选值, 而且候选值的个数比较小.

定理5.16　*设 E 和 E' 是 k 同种的椭圆曲线, 它们都是定义在域 k 上. 则 $|E_k| = |E_k'|$.*

证明 记 $\alpha=(\alpha_1,\alpha_2)$ 为 E 到 E' 的 k 同种映射, φ 和 φ' 分别为 E 和 E' 上的 Frobenius 自同态. 因为 α_1 的系数都在域 k 中, 则 $\alpha_1(X,Y)^q=\alpha_1(X^q,Y^q)$, 同样地也有 $\alpha_2(X,Y)^q=\alpha_2(X^q,Y^q)$. 因此

$$\varphi'\circ\alpha=\Big(\alpha_1(X,Y)^q,\quad \alpha_2(X,Y)^q\Big)=\Big(\alpha_1(X^q,Y^q),\quad \alpha_2(X^q,Y^q)\Big)=\alpha\circ\varphi.$$

如果 $\varphi^2-t\varphi+q=0$ 是 φ 的特征方程, 则有

$$0=\alpha\circ(\varphi^2-t\varphi+q)=\left(\varphi'^2-t\varphi'+q\right)\circ\alpha,$$

由命题 3.3 知 α 是满射, 故 $\varphi'^2-t\varphi'+q=0$. 再由定理 3.61 可知 $|E_k|=|E'_k|$. 事实上, 反之也是成立的, 可参阅 [Tate, 1966] 中的定理 1 (c). □

先假定 $p=2$ 或 $p=3$. 则 $j(E')=0$, 由定理 3.71 可知 E' 是超奇异椭圆曲线, 再由推论 3.73 及 $|E_k|=|E'_k|$ 知, E 也一定是超奇异的, 这一种情况已经在前面的测试中排除过了. 如果 $p>3$, 则有可能计算出 j 不变量为 0 或 1728 的椭圆曲线的个数, 这等同于在虚二次域 $\mathbb{Q}(i)$ 和 $\mathbb{Q}(\sqrt{-3})$ 中范数为 q 的元素 (参阅 [Müller, 1995] 的第 9.2 节). 同样地, 我们可以对随机选择的点, 测试相应的倍点运算, 看结果是否为 $\mathcal{O}$. 如果不是 $\mathcal{O}$, 则可以断言曲线 E 不 k 同种于 j 不变量为 0 或 1728 的椭圆曲线. 否则, 在 [Müller, 1995] 的第 11 章中给出的算法, 可以计算出该曲线的阶. 注意, 由第一章中对于密码体制安全性的描述可知, 我们并不需要知道整个群的阶, 只要知道一个充分大的循环子群的阶就够了, 而这个循环子群往往由一个随机点生成. 而上面的测试恰好可以检查随机点的阶. 如果找到了一个点, 它的阶能够被一个大素数整除, 那么就可以利用由该点生成的循环子群来构造密码体制, 而完全可以不用考虑这条椭圆曲线的阶是多少.

3. 计算 $t \bmod l$

如果前面两步的验证没有通过 (即所给的椭圆曲线不是超奇异的, 它的 j 不变量也等于 0 或 1728), 我们可以利用 5.4 和 5.5 节的方法, 对于奇素数 l 计算 $\tau_0\equiv t \pmod{l}$. 如果 l 是 Elkies 型素数, 可以计算出 τ_0 的确切值; 如果 l 是 Atkin 型素数, 则可以计算出最多为 $(l+1)/2$ 个可能的值. 对于 Elkies 型素数, 算法的复杂度由 Schoof 算法的 $O(\log^5 q)$ 个域运算 (参阅算法 5.8 的复杂度分析), 降到 $O(\log^3 q)$ 个域运算, 原因是所有的多项式计算是在模 f_C 的情况下进行的, 而 f_C 的次数为 $O(l)$ 而不是 Schoof 算法中的 $O(l^2)$. 注意, 由 5.4 节的分析可知, 利用同种映射计算 f_C 的算法复杂度不超过 $O(l^3)$.

对于 Elkies 型素数, 更进一步的工作是考虑素数的幂, 详细的情况可参阅 [Müller, 1995] 的第 8 章, [Couveignes and Morain, 1994] 或 [Couveignes et al., 1996].

对于 2 的幂，文献 [Couveignes and Morain, 1994] 的第 5 节讨论了 $p \neq 2$ 的情形，文献 [Menezes et al., 1996] 讨论了 $p = 2$ 的情形.

4. 部分信息的综合

令 $\mathcal{L}_1$ 表示 Elkies 素数集合 (或素数幂)，$\mathcal{L}_2$ 表示在上一步骤中考察的 Atkin 素数集，记

$$L_1 = \prod_{l\in\mathcal{L}_1}, \quad L_2 = \prod_{l\in\mathcal{L}_2} l, \quad L = L_1L_2,$$

由中国剩余定理能够计算出唯一的 t 模 L_1；模 L_2 却有多个可能的值. 具体地说就是，对于 Atkin 型素数 l，如果令 ν_l 表示 $t \bmod l$ 可能的值的个数，那么就有 $\prod_{l\in\mathcal{L}_2} \nu_l$ 个可能的 $t \bmod L_2$，从而也有这么多个可能的 $t \bmod L$，一般来说该值是 $|\mathcal{L}_2|$ 的幂.

下面需要判断哪一个关于 $|E_k|$ 的候选值是正确的，由定理 3.61，我们只需要考虑出现在 $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ 之间的候选值. 一般的做法如下：随机选取 E_k 上的一个点 P，用候选值做倍点运算，再检查是否为 $\mathcal{O}$. 如果只有一个值通过了测试，则这就是椭圆曲线 E_k 的阶. 否则的话①，就扩展集合 $\mathcal{L}_1$ 和 $\mathcal{L}_2$(即再计算一些 $t \bmod l$). 在实际情况中，当 $L > 4\sqrt{q}$ 时，第一个通过测试的值，往往就是正确的结果. Atkin 建议，这部分计算可采用大步–小步的算法来加快搜索速度，详细情况可参阅 [Müller, 1995] 的第 10.2 节或者 [Lercier, 1997a] 的第 11.2 节.

值得注意的是，由于有了 Atkin 型素数，则当 $|\mathcal{L}_2|$ 是 $\log q$ 的线性关系时，原来是多项式时间的 Schoof 算法，现在变成了指数时间的算法，而且如果我们选择 $\mathcal{L}_1 \cup \mathcal{L}_2$ 为最前面的素数集合时，则很可能就是这种情况. 然而，在实际计算中，这个多项式时间的算法速度反而更快.

5. 算法的实现

据我所知，有两个人公开发表了 SEA 算法的实现细节，当然椭圆曲线公钥密码的商业开发者，会独自处理他们的代码，我们无法得知他们的实现情况.

Lehmann, Maurer, Müller 和 Shoup 成功地计算出定义在特征是 425 位十进制素数的素数域上一条椭圆曲线的群阶，他们使用了 983 以下的所有小素数，并且测试了 $5 \cdot 10^6$ 个可能的候选值，花了 3000 多个小时. 详细可参阅 [Müller, 1995], [Lehmann, 1994], [Maurer, 1994] 和 [Lehmann et al., 1994] 等文献.

在文献 [Lercier, 1997a] 中，Lercier 提出了适用于任意特征的实现方法. 他的记录是计算出一条定义在 $\mathbb{F}_{2^{1301}}$ 的椭圆曲线的阶，花了 1200 多个小时，使用了 673

① 如果取 $L > 4\sqrt{q}$，则总能找到通过测试的候选值，因为至少 $|E_k|$ 一定能够通过检测 —— 译者注.

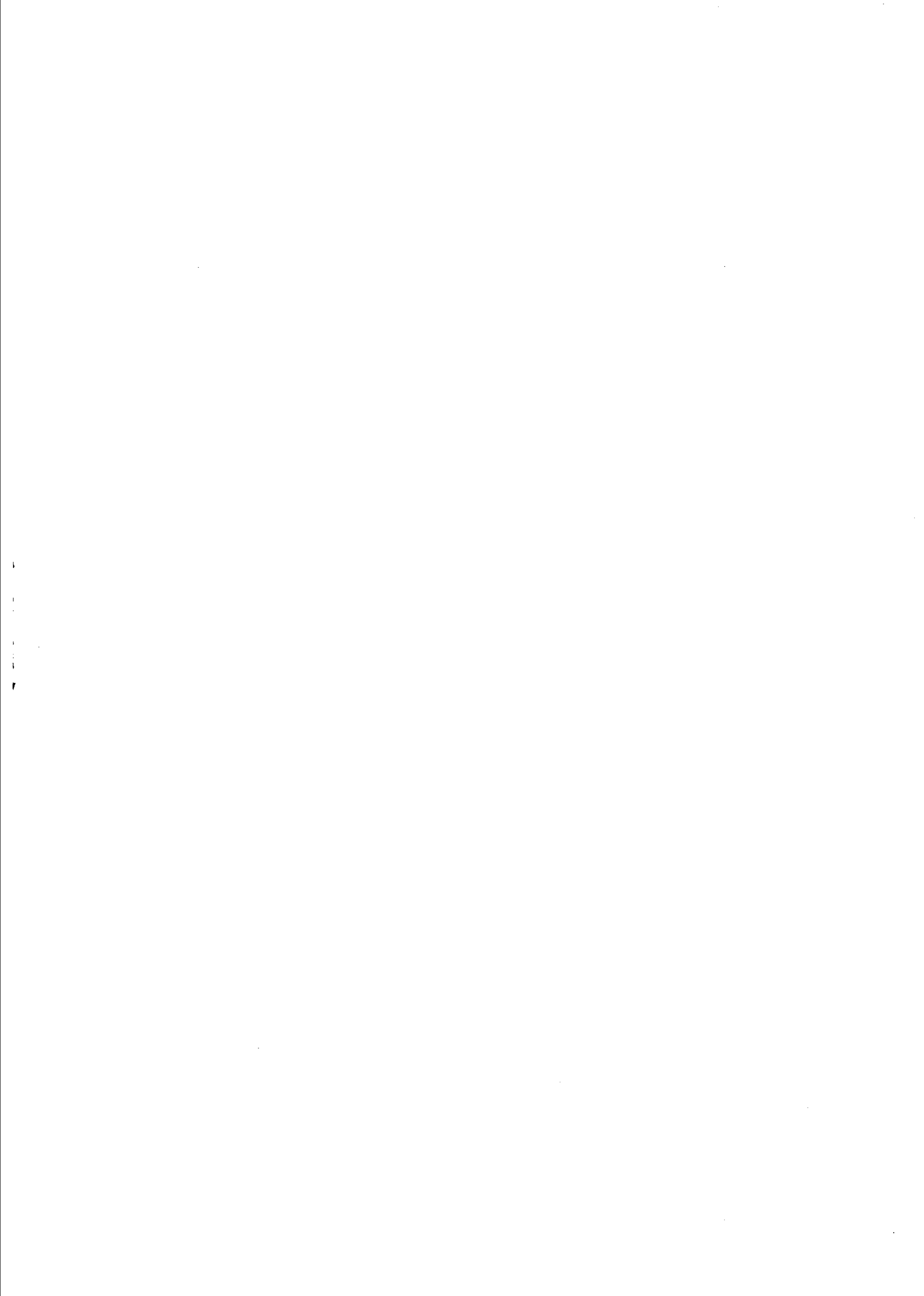
以下的所有小素数. 值得注意的是，算法的流程相当复杂，当计算了一个素数幂 l^k 之后，从原则上说还有三种可能的选择：

- 继续计算 l^{k+1},
- 处理下一个小素数,
- 停止计算 $t \bmod l$，综合已经得到的信息.

对于前面两个选择，Lercier 建议采用动态的策略，他为每一个可能的计算赋予一个整数，以刻画该计算所需要的代价，然后按照这个准则做出代价最小的选择.

上面的计算记录只是测试算法实现的极限. 由于运行时间需要数月 (当然可以利用昂贵的并行设备来减少运行时间)，这就使得这样大域上的椭圆曲线并不适用于经常使用的密码体制. 因此应该给出对于密码学来说常见大小的有限域上椭圆曲线的运算时间. 在密码学中通常建议使用的一个有限域是 $\mathbb{F}_{2^{155}}$，Lercier 在文献 [Lercier, 1997a] 中表 12.3 给出该域的运行时间是 90 秒 (90s). 这似乎很合理，但这样的计算需要不断重复，直至找到适合于密码算法的曲线. 事实上，为了避免在 4.3 节提出的 Pohlig-Hellman 攻击方法，$|E_k|$ 最好是素数，那么所有已知的关于离散对数问题的攻击手段都是指数级的，从而也就为大小为 2^{155} 的域提供了充分的安全性. 由于有限域特征的原因，椭圆曲线的阶中难免有小的素因子. 例如 $p = 2$，命题 3.41 和命题 3.38 表明非超奇异椭圆曲线的阶一定是 4 的倍数. Lercier 随机测试了这种类型的椭圆曲线，即形如 $Y^2 + XY = X^3 + a_6$ 的曲线，其 4 阶点是 $(\sqrt[4]{a_6}, \sqrt{6}) = \left(a_6^{2^{153}}, a_6^{2^{154}}\right)$，是否适合于密码学使用. 他采用了提前中止的策略，即一旦发现奇素数 l 或者 $l = 8$ 是 $|E_k|$ 的因子，则放弃这条椭圆曲线，他发现在 1000 条椭圆曲线中，只有 5 条适合于密码学应用，他花费的总时间是 250 分钟，详情可参阅 [Lercier, 1997a] 中表 12.6，或 [Lercier, 1997b].

我们可以得出这样的结论：寻找合适的随机的椭圆曲线还是比较困难的. 但是随着近年来算法方面的进展，这就使得寻找椭圆曲线在实际中变得可行，而且还提供了另外一种很有吸引力的选择 —— 使用特殊类型的椭圆曲线.



参考文献

Adleman, L. M. (1994). The function field sieve. In [*Adleman and Huang, 1994*], pages 108–121.

Adleman, L. M., DeMarrais, J., and Huang, M. D. (1994). A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In [*Adleman and Huang, 1994*], pages 28–40.

Adleman, L. M. and Huang, M. D., editors (1994). *Algorithmic Number Theory.* volume 877 of *Lecture Notes in Computer Science.* Berlin: Springer–Verlag.

ANSI(1998a). Agreement of symmetric keys on using Diffie-Hellman and MQV algorithms. Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9. 42–1998, American National Standards Institute. Available at http: //grouper. ieee. org/groups/1363/private/x9-42-10-02-98. zip.

ANSI(1998b). The elliptic curve digital signature algorithm(ECDSA). Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9. 62-1998, American National Standards Institute. Available at http: //grouper. ieee. org/groups/1363/private/x9-62-09-20-98. zip.

ANSI(1999). Key agreement and key transport using elliptic curve cryptography. Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9. 63-199x, American National Standards Institute. Available at http: //grouper. ieee. org/groups/1363/private/x9-63-01-08-99. zip.

Atkin, A. O. L. and Morain, F. (1993). Elliptic curves and primality proving. *Mathematics of Computation*, 61(203): 29–68.

Bézout, E. (1779). *Théorie Générale des Équations Algébriques.* Paris.

Blake, I. F., Fuji-Hara, R., Mullin, R. C., and Vanstone, S. A. (1984). Computing logarithms in finite fields of characteristic two. *SIAM J. Alg. Disc. Meth.*, 5(2): 276–285.

Brent, R. P. (1980). An improved Monte Carlo factorization algorithm. *BIT*, 20: 176–184.

Brickell, E. F., editor(1993). *Advances in Cryptology—CRYPTO'92.* volume 740 of *Lecture Notes in Computer Science*, Berlin: Springer–Verlag.

Buell, D. A. and Teitelbaum, J. T., editors(1998). *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L Atkin,* volume 7 of *Studies in Advanced Mathematics.* American Mathematical Society.

Certicom(1997). ECC challenge. http: //www. certicom. com/chal/index. htm.

Charlap, L. S. and Robbins, D. P. (1998). An elementary introduction to elliptic curves. CRD Expository Report 31, Institute for Defense Analyses, Princeton.

Cohen, H. (1993). A *Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. New York: Springer-Verlag.

Cohen, H., editor (1996). *Algorithmic Number Theory. —ANTS–II*, volume 1122 of *Lecture Notes in Computer Science.* Berlin: Springer-Verlag.

Commission of the European Communities(1998). Proposal for a European parliament and council directive on a common framework for electronic signatures. Technical report, European Union. A vailable in all languages of the European Union; in english at http: //europa. eu. int/comm/dg15/en/media/infso/com297en. pdf.

Coppersmith, D. (1984). Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory,* 30(4): 587–594.

Couveignes, J. M. (1994). *Quelques calculs en théorie des nombres.* PhD thesis, Université de Bordeaux I. Available at http: //www. ufr-mi. u-bordeaux. fr/~ couveign/Publi/ Cou94-4. ps.

Couveignes, J. M. (1996). Computing l-isogenies with the p-torsion. Preprint; available at http: //www. ufr-mi. u-bordeaux. fr/~ couveign/Publi/Cants96. ps.

Couveignes, J. M., Dewaghe, L., and Morain, F. (1996). Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Technical Report LIX/RR/96/03, Laboratoire d'Informatique de l'Ecole Polytechnique (LIX), Palaiseau. A vailable at ftp: //lix.polytechnique. fr/pub/ submissions/morain/Preprints/isogcycles. ps. Z.

Couveignes, J. M. and Morain, F. (1994). Schoof's algorithm and isogeny cycles. In [*Adleman and Huang, 1994*]: 43–58.

Deuring, M. (1941). Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem mathematischen Seminar der hamburgischen Universität,* 14: 197–272.

Diffie, W. and Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory,* 22(6): 644–655.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory,* 31(4): 469–472.

Elkies, N. D. (1998). Elliptic and modular curves over finite fields and related computational issues. In [*Buell and Teitelbaum, 1998*], pages 21–76.

Enge, A. (1998). Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. Submitted to *Mathematics of Computation.*

Escott, A. (1998). Implementing a parallel Pollard rho attack on ECC. Transparencies of the presentation given at the 2nd Workshop on Elliptic Curve Cryptography at the University of Waterloo; available at http: //cacr. math. uwaterloo. ca/escott. ps. zip.

Frey, G. and Rück, H. G. (1994). A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves . *Mathematics of Computation,* 62(206): 865–874.

Fulton, W. (1969). *Algebraic Curves.* Mathematics Lecture Note Series. The Benjamin/ Cum-mings Publishing Company, Reading(Massachusetts).

Fumy, W., editor(1997). *Advances in Cryptology——EUROCRYPT'97,* volume 1233 of *Lecture Notes in Computer Science.* Berlin: Springer-Verlag.

Gallant, R., Lambert, R., and Vanstone, S. (1998). Improving the parallelized Pollard lambda search on binary anomalous curves. Preprint.

Gauβ, C. F. (1801). *Disquisitiones Arithmeticae.* Gerh. Fleischer Jun., Leipzig.

Gillings, R. J. (1972). *Mathematics in the Time of the Pharaohs.* MIT Press, Cambridge (Massachusetts).

Gordon, D. M. (1993). Discrete logarithms in $GF(p)$ using the number field sieve. *SIAM Journal on Discrete Mathematics,* 6(1): 124–138.

Gordon, D. M. and McCurley, K. S. (1993). Massively parallel computation of discrete logarithms. In [*Brickell, 1993*], pages 312–323.

Hall Jr., M. (1959). *The Theory of Groups.* New York: Macmillan.

Hasse, H. (1934). Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abhandlungen aus dem mathematischen Seminar der hamburgischen Universität,* 10: 325–348.

Husemöller, D. (1987). *Elliptic Curves.* Graduate Texts in Mathematics. New York: Springer-Verlag.

IEEE(1998). Standard specifications for public key cryptography. Technical Report P1363/ D8(Draft Version 8), Institute of Electrical and Electronics Engineering. A vailable at http: //grouper. ieee. org/groups/1363/index. html.

Jacobson, M. J., Koblitz, N., Silverman, J. H., Stein, A., and Teske, E. (1999). Analysis of the xedni calculus attack. Preprint.

Johnson, D. S., Nishizeki, T., Nozaki, A., and Wolf, H. S., editors(1987). *Discrete Algorithms and Complexity, Proceedings of the Japan-US Joint Seminar, June 4-6, 1986, Kyoto, Japan, volume* 15 of *Perspectives in Computing.* Orlando: Academic Press.

Knuth, D. E. (1981). *The Art of Computer Programming* , volume 2-Seminumerical Algorithms. Addison-Wesley, Reading(Massachusetts), 2nd edition.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation,* 48(177): 203–209.

Koblitz, N. (1991), Constructing elliptic curve cryptosystems in characteristic 2. In [*Menezes and Vanstone, 1991*]: 156–167.

Koblitz, N. (1993). *Introduction to Elliptic Curves and Modular Forms.* Graduate Texts in Mathematics. New York: Springer-Verlag, 2nd edition.

Koblitz, N. (1994). *A Course in Number Theory and Cryptography.* Graduate Texts in Mathematics. New York: Springer-Verlag, 2nd edition.

Koblitz, N. (1998). *Algebraic Aspects of Cryptography,* volume 3 of *Algorithms and Computations in Mathematics.* Berlin: Springer-Verlag.

Lang, S. (1978). *Elliptic Curves: Diophantine Analysis,* volume 231 of *Grundlehren der mathematischen Wissenschaften.* Berlin: Springer-Verlag.

Lang, S. (1987). *Elliptic Functions.* Graduate Texts in Mathematics. New York: Springer-Verlag, 2nd edition.

Lay, G.-J. and Zimmer, H. G. (1994). Constructing elliptic curves with given group order over large finite fields . In [*Adleman and Huang, 1994*]: 250–263.

Lehmann, F., Maurer, M., Müller, V., and Shoup, V. (1994). Counting the number of points on elliptic curves over finite fields of characteristic greater than three. In [*Adleman and Huang, 1994*]: 60–70.

Lehmann, F. J. (1994). Implementierung von Algorithmen zur Berechnung modularer Polynome und deren Anwendung im Algorithmus von Atkin. Master's thesis, Universität des Saarlandes, Saarbrücken. Available at ftp: //ftp. informatik. tu-darmstadt. de/pub/TI/reports/lehmann. diplom. ps. gz.

Lercier, R. (1996). Computing isogenies in $GF(2^n)$. In [*Cohen, 1996*]: 197–212.

Lercier, R. (1997a). *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, École polytechnique, Palaiseau. A vailable at ftp: //lix. polytechnique. fr/pub/lercier/papers/these. ps. Z.

Lercier, R. (1997b). Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$. In [*Fumy, 1997*]: 379–392.

Lercier, R. and Morain, F. (1996). Algorithms for computing isogenies between elliptic curves. To appear in Computational Perspectives on Number Theory, 1997; available at ftp: //lix. polytechnique. fr/pub/submissions/morain/Preprints/isogenies. ps. Z and ftp: //lix. polytechnique. fr/pub/lercier/papers/isogenies: ps. Z.

Lewis, D., editor(1971). *Proceedings of Symposia in Pure Mathematics,* volume 10, Providence(Rhode Island). American Mathematical Society.

Lovorn Bender, R. (1999). Rigorous, subexponential algorithms for discrete logarithms in $GF(p^2)$. To appear in *SIAM J. Discrete Math.*

Martin, R. and McMillen, W. (1997). An elliptic curve over $\mathbb{Q}$ with rank at least 23. Posting to the Number Theory List, see http: //listserv.nodak.edu/archives/nmbrthry. html.

Maurer, M. (1994). Eine Implementierung des Algorithmus von Atkin zur Berechnung der Punktanzahl elliptischer Kurven über endlichen Primkörpern der Charakteristik größer

drei. Master's thesis, Universität des Saarlandes, Saarbrücken. Available at ftp: //ftp. informatik. tu darmstadt. de/pub/TI/reports/maurer. diplom. ps. gz.

Maurer, U. M. and Wolf, S. (1996). On the complexity of breaking the Diffe-Hellman protocol. Technical Report 244, Institute for Theoretical Computer Science, ETH Zürich. Available at ftp: //ftp. inf. ethz. ch/pub/publications/-papers/ti/isc/Diffie_Hellman_DL_TR. ps. gz.

McCurley, K. S. (1989). Cryptographic key distribution and computation in class groups. In [*Mollin, 1989*]: 459–479.

Menezes, A., editor (1993a). *Applications of Finite Fields.* Kluwer Academic Publishers, Boston/Dordrecht/London.

Menezes, A. (1993b). *Elliptic Curue Public Key Cryptosystems.* Kluwer Academic Publishers, Boston/Dordrecht/London.

Menezes, A. and Vanstone, S. (1990). Isomorphism classes of elliptic curves over finite fields of chatacteristic 2. *Utilitas Mathematica,* 38: 135–153.

Menezes, A. J., Okamoto, T., and Vanstone, S. A. (1993a). Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory,* 39(5): 1639-1646.

Menezes, A. J., Oorschot, P., and Vanstone, S. A. (1997). *Handbook of Applied Cryptography.* CRC Press, Boca Raton.

Menezes, A. J. and Vanstone, S. A., editors (1991). *Advances in Cryptology—CRYPTO'90,* volume 537 of *Lecture Notes in Computer Science.* Berlin: Springer-Verlag.

Menezes, A. J., Vanstone, S. A., and Zuccherato, R. J. (1993b). Counting points on elliptic curves over F_{2^m}. *Mathematics of Computation,* 60(201): 407–420.

Mestre. J. F. (1982). Construction d'une courbe elliptique de rang⩾12. *Comptes Rendus des Séances de l'Académie des Sciences de Paris, Série I,* 295: 643–644.

Mestre, J. F. (1986). Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Mathematica,* 58: 209–232.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In [*Williams, 1986*], pages 417–426.

Mollin, R. A., editor(1989). *Number Theory and Applications,* volume 265 of *NATO ASI Series C: Mathematical and Physical Sciences.* Dordrecht: Kluwer Academic Publishers.

Morain, F. (1997). Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique ⩾ 3. *Utilitas Mathematica,* 52: 241–253.

Müller, V. (1991). Die Berechnung der Punktanzahl von elliptischen Kurven über endlichen Primkörpern. Master's thesis, Universität des Saarlandes, Saarbrücken. Available at ftp: // ftp. informatik. tu-darmstadt. de/pub/TI/reports/vmueller. diplom. ps. gz.

Müller, V. (1995). *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kuruen über endlichen Körpern der Charakteristik größer drei.* PhD thesis, Universität des Saarlandes, Saarbrücken. Available at ftp://ftp. informatik. tu–darmstadt. de/pub/TI/ reports/vmueller. diss. ps. gz.

Müller, V., Stein, A., and Thiel, C. (1997). Computing discrete logarithms in real quadratic congruence function fields of large genus. To appear in Mathematics of Computation; available at http://www. informatik. tu-darmstadt. de/TI/Mitarbeiter/vmueller/ffdl. ps. gz.

NIST(1994). Digital signature standard(DSS). Federal Information Processing Standard Publication 186, National Institute of Standards and Technology. Available at http: //csrc. nist. gov/fips/fips 186. ps.

NIST(1995). Secure hash standard. Federal Information Processing Standard Publication 180-1, National Institute of Standards and Technology. Available at http: //csrc. nist. gov/fips/fip 180-1. ps.

NIST(1998). Digital signature standard(DSS). Federal Information Processing Standard Publication 186-1, National Institute of Standards and Technology. Available at http: //csrc. nist. gov/fips/fips1861. pdf.

Ohta, K. and Pei, D., editors(1998). *Advances in Cryptology——ASIACRYPT'98*, volume 1514 of *Lecture Notes in Computer Science.* Berlin: Springer-Verlag.

Oorschot, P. and Wiener, M. J. (1999). Parallel collision search with cryptanalytic applications. *Journal of Cryptology,* 12(1): 1–28.

Pohlig, S. C. and Hellman, M. E. (1978). An improved algorithm for computing logarithms over *GF(P)*and its cryptographic significance. *IEEE Transactions on Information Theory,* 24(1): 106–110.

Pollard, J. M. (1978). Monte Carlo methods for index computation(mod p). *Mathematics of Computation,* 32(143): 918–924.

Pomerance, C. (1987). Fast, rigorous factorization and discrete logarithm algorithms, In [*Johnson et al., 1987*]: 119–143.

Rosser, J. B. and Schoenfeld, L. (1962). Approximate formulas for some functions of prime numbers, *Illinois Journal of Mathematics,* 6: 64–94.

Rück, H. G. (1987). A note on elliptic curves over finite fields. *Mathematics of Computation,* 49(179): 301–304.

Satoh, T. and Araki, K. (1998). Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Mathematici Universitatis Sancti Pauli,* 47(1): 81–92.

Schirokauer, O. (1993). Discrete logarithms and local units. *Philosophical Transactions Royal Society London A,* 345: 409–423.

Schnorr, C. P. and Lenstra Jr., H. W. (1984). A Monte Carlo factoring algorithm with linear storage. *Mathematics of Computation*, 43(167): 289–311.

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170): 483–494.

Schoof, R. (1987). Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory*, A 46: 183–211.

Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7: 219–254.

Semaev, I. A. (1998). Evaluation of discrete logarithms in a group of p–torsion points of an elliptic curve in characteristic p. *Mathematics of Computation*, 67(221): 353–356.

Shafarevich, J. R. (1974). *Basic Algebraic Geometry*. Die Grundlehren der mathematischen Wissenschaften. Berlin: Springer-Verlag.

Shanks, D. (1971). Class number, a theory of factorization and genera. In [*Lewis, 1971*]: 415–440.

Shoup, V. (1997). Lower bounds for discrete logarithms and related problems. In [*Fumy, 1997*]: 256–266.

Silverman, J. H. (1986). *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. New York: Springer-Verlag.

Silverman, J. H. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. New York: Springer-Verlag.

Silverman, J. H. (1998). The xedni calculus and the elliptic curve discrets logarithm problem. Preprint; available at http: //www. math. brown. edu/~jhs/Preprints/ XedniCalculus. ps. gz.

Silverman, J. H. and Suzuki, J. (1998). Elliptic curve discrete logarithms and the index calculus. In [*Ohta and Pei, 1998*]: 110–125.

Smart, N. P. (1999). The discrete logarithm problem on elliptic curves of trace one. To appear in Journal of Cryptology.

Stinson, D. R. (1995). *Cryptography——Theory and Practice*. Discrete Mathematics and its Applications. Boca Raton: CRC Press.

Tate, J. (1966). Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2: 134–144.

Teske, E. (1998). Better random walks for Pollard's rho method. Technical Report CORR98-52, Centre for Applied Cryptographic Research, University of Waterloo. Available at http: // cacr. math. uwaterloo. ca/techreports/1998/-corr98-52. ps.

UNCITRAL (1998a). Draft uniform rules on electronic signatures. Technical Report A/CN. 9/WG. IV/WP. 79, United Nations Commission on International Trade Law. Available at http: //www. un. or. at/uncitral/english/sessions/wg_ etc/wp-79. htm.

UNCITRAL (1998b). Electronic signatures. Technical Report A/CN. 9/WG. IV/WP. 80, United Nations Commission on International Trade Law. Available at http: //www. un. or. at/uncitral/english/sessions/wg- ec/wp-80. htm.

Vélu, J. (1971). Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris, Série A,* 273: 238–241.

Waterhouse, W. C. (1969). Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure,* 4e *Série,* 2: 521–560.

Weber, D. (1996). Computing discrete logarithms with the general number field sieve. In [*Cohen, 1996*]: 391–403.

Wiener, M. J. and Zuccherato, R. J. (1998). Faster attacks on elliptic curve cryptosystems. In *Proceedings of SAC, Workshop on Selected Areas in Cryptography, Lecture Notes in Computer Science.*

Williams, H. C., editor (1986). *Advances in Cryptology——CRYPTO'85,* volume 218 of *Lecture Notes in Computer Science.* Berlin: Springer-Verlag.

符 号 表

Γ	因子基
Δ	E 的判别式
Φ_l	l 次模多项式
α	$p^2/\mid E[p]\mid, p\in\{2,3\}$
α_m	α 在 $E[m]$ 上的限制
κ	$E\to \mathrm{Pic}^0(E)$
λ	周期
μ	前周期
σ	$\mathrm{Pic}^0(E)\to E$
τ_Q	关于 Q 点的平移映射
φ	Frobenius 自同态
χ	二次特征
ψ_m	m 次除子多项式
$[0]$	$E_{K(E)}$ 上的无穷远点
$A^2(K)$	K 上的仿射平面
$\mathcal{B}$	$\{iP \mid 0\leqslant i<s\}$
$\mathcal{C}$	密文空间
Dg_m	g_m 的导数
Dh_m	h_m 的导数
$\mathrm{Div}(E)$	E 的除子群
$\mathrm{Div}^0(E)$	零次除子群
$\langle E[m]\rangle$	$\sum_{P\in E[m]}\langle P\rangle$
$\mathrm{End}(E)$	E 上的自同态环
$\mathcal{G}$	$\{jsP : 0\leqslant j<s\}$
$G[n]$	群 G 中所有 n 阶扭元素构成的集合
$G[n^\infty]$	$\bigcup_{i=0}^{\infty} G[n^i]$
$H(\Delta)$	Δ 的 Kronecker 类数符号
$\mathcal{K}$	密钥空间
$K(C)$	曲线 C 的有理函数域
$K[C]$	曲线 C 的坐标环
$K[X,Y,Z]_{\mathrm{hom}}$	齐次多项式的全体
$\mathcal{M}$	明文空间

N	范函数
$N(t)$	迹为 t 的非同构椭圆曲线的数目
$\mathcal{O}$	无穷远点
$\mathcal{O}_P(C)$	C 在 P 点的局部环
$P^2(K)$	K 上的射影平面
P^*	P 的齐次化
P_*	P 的非齐次化
$\mathrm{Pic}(E)$	E 的除子类群
$\mathrm{Pic}^0(E)$	除子类群的零次部分
Tr	迹函数
deg	次数
$\mathrm{div}r$	有理函数 r 的除子
e_m	m 扭点的 Weil 对
$e_{[m]}$	$[m]$ 的分歧指数
e_φ	Frobenius 自同态 φ 的分歧指数
e_{τ_Q}	平移映射 τ_Q 的分歧指数
g_T	除子为 $[m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)$ 的有理函数,
g_m	$[m] = (g_m, h_m)$
h_m	$[m] = (g_m, h_m)$
j/C	E/C 的 j 不变量
$l(r)$	r 在 $\mathcal{O}$ 处的首项系数
$[m]$	m 乘映射
$\mathfrak{m}_P(C)$	局部环 $\mathcal{O}_P(C)$ 的极大理想
$\|\Delta\|$	除子 Δ 的范数
$\mathrm{ord}_P(r)$	r 在 P 点的阶
$\mathrm{Prin}(E)$	主除子群
$\Delta_1 \sim \Delta_2$	除子 Δ_1, Δ_2 线性等价
$E[m]$	全体 m 扭点
$e_\alpha(P)$	α 在 P 点出的分歧指数
$K(C^*)$	有理函数域
$L[\alpha, c]$	$O\left(e^{(c+o(1))(\log n)^\alpha(\log\log n)^{1-\alpha}}\right)$

中英文对照索引

《现代数学译丛》已出版书目

(按出版时间排序)

1　椭圆曲线及其在密码学中的应用——导引　2007. 12　〔德〕Andreas Enge 著　吴　铤　董军武　王明强　译

2　金融数学引论——从风险管理到期权定价　2008. 1　〔美〕Steven Roman 著　邓欣雨　译

(O-2913.0101)



ISBN 978-7-03-020034-1

9 787030 200341 >

定 价：38.00 元